Андрей Синельников

ШИФРЫ СОВЕТСКОЙ РАЗВЕДКИ

Оглавление:

Шифр Рамзая.

Шифры тоже сражались!

Там за океаном...

Марк, Вик и пять центов.

Шифры агентов ЦРУ.

Шифры никогда не были и, понятно, не станут обычными абстрактными вещами. Но, являясь важнейшей составной частью системы безопасности любого государства, они по природе своей вынуждены пребывать в безвестности. История нынешней криптографии, и её влияние на современность – очевидно, удел будущих историков. Но настоятельно важно знать, уважать и помнить своё прошлое любому поколению нашей страны. И задача автора – хоть в небольшой степени рассказать о великой «битве шифров» XX века, в которой советские шифровальщики и разведчики принимали самое непосредственное участие.

И в которой нам тоже есть, чем гордиться!

От автора

Для подготовки этого очерка я пользовался доступными в прессе материалами о многих американских агентах. И все время ловил себя на мысли, что пишу как будто про одного единственного шпиона. Настолько они все похожи и одинаковы. И удивительно скучны. Американцы плодили им свои инструкции под копирку,

уверяя каждого в отдельности, что думают только о безопасности агента. Но подобная шаблонность вряд ли вела к этой самой безопасности. Об этом говорит печальная судьба каждого из шпионов. И если бы они знали, что их непробиваемые шифры срисованы ЦРУ-шниками с шифров великих советских разведчиков, то, наверное, расстроились бы. Представить Гузенко, Попова, Хейханена, Пеньковского, Нилова, Огородника, Толкачева, Поташова, Полякова, Гордиевского и прочих «любителей» Родины в одном ряду с Зорге, Радо, Треппером, Абелем, Филби, Блейком и с десятками других советских разведчиков совершенно невозможно. Поэтому первые – обычные, презираемые всеми изменники, а героизм вторых удивлял и удивляет весь мир.

Библиография:

1. Шифр ВИК http://www.quadibloc.com/crypto/pp1324.htm
2. Шифр Зорге http://refpeed.net/dokeos/courses/INFO4d3ea/document/pdf/cryptunit7.pdf?cidReq=INFO469bc
3. Джеймс Донован, «Незнакомцы на мосту», М., 1992.
4. Де Си Грамон, «История шпионажа», Смоленск, 2002.
5. Дэвид Кан, «Взломщики кодов», М., 2000.
6. Лев Лайнер, «Венона» - самая секретная операция американских спецслужб», М.,2003.
7. Соболева Т.А., «История шифровального дела в России», М., 2002.
8. Хайнц Хене, «Пароль: Директор», Терра, 2003.
9. Синельников А.В., «***Шифры и революционеры России***», 2000. http://www.hrono.ru/libris/lib_s/shifr00.html

Новосибирск, январь 2008 года

Здесь читайте:

"Лица в штатском" (биографический указатель).

Судоплатов П.А. **Спецоперации. Лубянка и Кремль 1930-1950 годы**.

СТАТЬИ НА ИСТОРИЧЕСКИЕ ТЕМЫ

Проект ХРОНОС существует с 20 января 2000 года,

на следующих доменах:
www.hrono.ru
www.hrono.info
www.hronos.km.ru,

Редактор Вячеслав Румянцев

Андрей Синельников

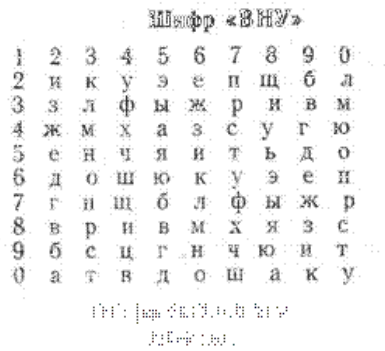
ШИФРЫ СОВЕТСКОЙ РАЗВЕДКИ

Шифр Рамзая

Рихарду Зорге в истории нашей Родины суждено было занять особое место. Волею судьбы и благодаря своим исключительным человеческим качествам он поднялся на самую вершину Олимпа, под названием Советская разведка. Десятки книг, сотни статей, документальные и художественные фильмы, улицы, названные в честь великого разведчика. Но, собирая материалы о нём, я, за редким исключением, не мог обнаружить в отечественной литературе никаких правдивых материалов о шифре его разведгруппы. Как, впрочем, и о шифрах других легендарных его товарищей – Леопольда Треппера, Шандора Радо, Рудольфа Абеля. А, между тем, история их шифров – одна из захватывающих страниц криптографии XX века. Здесь нам есть, чем гордиться. «Триумфом советской разведки» назвал её агентурные шифры известный американский историк Дэвид Кан. Давайте же перелистаем доступные ныне страницы истории, заглянем в святая святых наших выдающихся разведчиков. Именно советские шифры, разработанные, несомненно, замечательными специалистами своего дела, на десятилетия определили вектор развития мировой криптографии в области так называемых «ручных шифров». И этот факт со всей очевидностью вытекает из содержания моих коротких очерков.

Рихард Зорге

Идея подобных шифров давно известна, но была доведена советскими шифроаналитиками до совершенства! Первой его частью являлся так называемый квадратный (шахматный) шифр, наложенный затем на иные способы тайнописи. Появление таких двойных шифров зарубежные исследователи относят к российским революционерам, называя их «шифром нигилистов». Но вряд ли это корректно. Ибо сами революционеры в свою очередь воспользовались криптографическими идеями, возникшими задолго до них. Так шахматный шифр берет своё начало со знаменитого «полибианского квадрата», а вторая составляющая шифра носила среди российских подпольщиков название «гамбеттовского ключа» в честь известного премьер-министра Франции XIX века Л. Гамбетты.



Наиболее близко идея будущего знаменитого шифра советских разведчиков изложена в исследовании революционера П. Розенталя «Шифрованное письмо», изданном ещё в 1904 году. Но говорить, что эта работа дала толчок распространению аналогичных шифросистем среди всего российского подполья не приходится. Вплоть до самого Октябрьского переворота 1917 года шифры революционеров оставались достаточно простыми. Впрочем, и долгое время после революции системы тайнописи советских разведчиков были такими же несложными и только к середине 30-х годов (после ряда их громких провалов) они стали приобретать свой законченный вид.

И шифр Рихарда Зорге (руководителя японской резидентуры ГРУ «Рамзай») о котором здесь пойдёт речь, нужно рассматривать как типовой образец действующих шифросистем всех советских спецслужб, а не приписывать его изобретение несправедливо самому Зорге или искать в нём некую уникальность. Свои телеграммы в Москву Зорге для конспирации составлял преимущественно на английском языке. Поэтому в качестве ключа для построения квадратного шифра было выбрано слово **«SUBWAY»**, что переводится как «подземный ход». Не правда ли, достаточно символично для разведчика?

Ключ выписывался в верхней строке квадратной таблички. А в оставшиеся клетки по порядку проставлялись буквы английского алфавита, не вошедшие в слово SUBWAY. Таким образом, мы получим следующую сетку:

S	**U**	**B**	**W**	**A**	**Y**
c	d	E	f	g	h
I	j	k	L	m	N
O	p	q	R	T	v
x	z	.	/		

В конце алфавита в таблице добавлено два знака. Это точка (.) и знак индикатора (/) - для обозначения разделителя слов или перехода на цифровой текст. Но об этом, подробнее, ниже.

Однако таблица в подобном виде использовалась только для придания вошедшим в нее символам новых цифровых обозначений.

Известно, что наиболее часто встречаемые в английской речи восемь букв можно представить в виде анаграммы ASINTOER (фраза "a sin to err" («грех в заблуждении») без последней буквы). Её то и использовал Зорге в качестве второго шага построения своего шифра. Для этого он нумеровал входящие в анаграмму буквы в своей табличке по порядку сверху вниз и получал новую таблицу:

S= 0	U	B	W	A=5	Y
c	d	E=3	f	g	h
I =1	j	k	L	m	N=7
O =2	p	q	R=4	T=6	v
x	z	.	/		

Конечной целью разведчиков являлось составление следующего квадратного шифра:

	0	1	2	3	4	5	6	7	8	9
-	s	i	o	e	r	a	t	n	-	-
8	c	x	u	d	j	p	z	b	k	q
9	.	w	f	L	/	g	m	y	h	v

Понять систему его построения нетрудно. В верхней строке мы видим наиболее встречаемые в английском языке буквы, которым даны цифровые обозначения от 0 до 7. В две оставшиеся строки выписаны по порядку остальные буквы из таблицы «SUBWAY» (то же сверху вниз). Они получают обозначения в виде двоичных чисел от 80 до 99. Как видно, в верхней строке конечные клетки под номерами 8 и 9 пустые. Эти цифры становятся номерами строк в ключевой таблице. Таким образом, здесь мы имеем воплощение идеи так называемого пропорционального шифра, позволяющее резко уменьшить количество входящих в шифрограмму знаков. В зависимости от размера текста это сокращение доходило до 30%. А это было очень важно для облегчения самого процесса шифровки, затруднения возможной дешифровки противником и уменьшения времени передачи радиограмм. Отделение же в тексте однозначных знаков от двузначных (конечно, при знании кодовой таблицы) не представляет никаких трудностей. Это была великолепная идея неизвестного нам советского криптолога, нашедшая затем в мировой криптографии широкое распространение.

Предположим, нужно зашифровать следующую телеграмму на немецком языке: «DAL. DER SOWJETISCHE FERNE OSTEN KANN ALS SICHER VOR EINEM ANGRIFF JAPANS ERACHTET WERDEN. RAMSAY» [DAL. Советский Дальний Восток может не опасаться нападения Японии. Рамзай.] Каждая радиограмма разведчиков начиналась их «обратным адресом»: DAL. Это были начальные буквы географического названия Дальний Восток. Заменяя буквы, знаки препинания и добавляя разделитель согласно квадратного шифра Зорге, получим:

DAL .DE R/SO WJE TISC HE/ FERN E/OS TEN/ KANN /AL S/SI CHE R/V OR/E INEM /ANG RIF F/J APA NS/E RACH TET/ WER DEN. RAM SAY .

83593 90833 49402 91843 61080 98394 92347 39420 63794 88577 94593 09401 80983 49499 24943 17396 94579 54192 92948 45855 70943 45809 86369 49134 83379 04596 05979 0

Имея ввиду, что шифротекст разведчики разбивали на 5-ти значные группы, последние цифры криптограммы или дополняли до полной пятёрки нулями, или просто удаляли.

Здесь мы подошли к главному секрету Рамзая. Первоначальная шифровка текста далее перекодировалась методом наложения на него бесконечной одноразовой цифровой гаммы по модулю 10. Способ получения её мог быть абсолютно разным: начиная от использования так называемых одноразовых шифровальных блокнотов до преобразования букв определенного книжного текста в цифры. И тот, и другой способ имели в разведке самое широкое применение и мы это еще увидим. Но для Зорге задачу значительно упростили. В качестве шифровальной книги был выбран толстенный «Немецкий статистический ежегодник за 1935 год», состоящий из сотен числовых таблиц, из которых наугад и выбиралась требуемые гаммы.

Предполагалось, что наличие у разведчиков в Японии подобного справочника никак не могло навести на подозрения. Ведь Р. Зорге был известным немецким журналистом, а его главный помощник и радист М. Клаузен – бизнесменом. Конечно, цифровые последовательности, получаемые с помощью этих таблиц, не были достаточно равномерными. В них неизбежно преобладали некоторые цифры, что вело к их повторению. Тем не менее, такие гаммы имели достаточное разнообразие, и никогда не были успешно преодолены вражескими криптоаналитиками.

Первая половина ежегодника на белой бумаге содержала статистические данные о Германии. Эта часть книги использовалась в качестве основы для кодирования шифрограмм непосредственно самой резидентурой Зорге. Во второй части справочника, на листах зеленого цвета, приводились международные статистические обзоры: ею уже пользовался московский Центр для шифровки ответных радиограмм. Это разделение делалось для предотвращения возможного наложения одинаковых гамм при шифровании текстов в Токио и Москве, что прямо могло привести к дешифровке радиограмм противником. Очевидно, что и сам Зорге и его помощник должны были делать в тексте своей кодовой книги какие-то пометки для недопущения всё того же повтора ключа. При аресте в 1941 году в квартирах Р. Зорге и М. Клаузена японской полицией были обнаружены совершенно одинаковые справочники с подозрительными отметками. Что сразу навело контрразведку на ключевую книгу пойманных шпионов.

Итак, цифры гаммы поочередно выбирались из справочника и выписывались под цифрами шифротекста, затем шло по-значковое сложение цифр клера и ключа по модулю 10. То есть, при сложении цифр во внимание принимались только единицы суммы, а десятки отбрасывались.

Клер:	83593	90833	49402	91843	61080	98394	92347	39420	63794	88577	94593	09401	80983	49499
Гамма:	35635	51303	24932	10010	78191	12106	21169	41861	76147	10589	66984	85249	50397	01471
Шифр:	**18128**	**41136**	**63334**	**01853**	**39171**	**00490**	**13406**	**70281**	**39831**	**98056**	**53477**	**84640**	**30270**	**40860**

	24943	17396	94579	54192	92948	45855	70943	45809	86369	49134	83379	04596	05979	
	03330	91929	56622	01806	15112	84112	13865	86318	09150	65213	43724	38399	27273	
	27273	**08215**	**40191**	**55998**	**07050**	**29967**	**83708**	**21117**	**85419**	**04347**	**26093**	**32885**	**22142**	

4. Schiffsverkehr über See
e. Verkehr in den wichtigeren deutschen Häfen

Im Jahre	Angekommene Schiffe: mit Ladung		in Ballast oder leer		davon zusammen im Auslandverkehr		Abgegangene Schiffe: mit Ladung		in Ballast oder leer		davon zusammen im Auslandverkehr	
	Anzahl	in 1 000 Reg.-Tons netto	Anzahl	in 1 000 Reg.-Tons netto	Anzahl	in 1 000 Reg.-Tons netto	Anzahl	in 1 000 Reg.-Tons netto	Anzahl	in 1 000 Reg.-Tons netto	Anzahl	in 1 000 Reg.-Tons netto
1913	187	92	—	—	91	62	46	11	27	8	25	6
1933	352	168	2	3	219	124	150	65	8	4	103	51
1934	308	147	—	—	190	107	161	76	4	2	112	57
1913	294	418	46	4	252	412	176	23	183	340	181	333
1933	183	147	36	16	37	100	126	27	69	95	81	84
1934	195	186	69	23	107	181	230	114	86	79	122	96
1913	253	63	14	1	113	56	35	5	130	32	49	32
1933	100	107	81	9	112	106	211	69	41	86	176	147
1934	105	89	66	9	86	85	249	50	39	70	147	103
1913	3 309	1 929	566	220	1 806	1 511	2 841	1 213	865	863	1 809	1 506
1933	5 213	4 372	436	399	2 727	3 343	4 692	4 322	876	497	3 256	3 703
1934	5 372	4 715	773	739	3 062	3 819	5 433	4 940	802	571	3 718	4 239
1913	1 414	2 280	50	78	554	2 038	1 537	2 231	112	183	502	1 963
1933	976	2 514	68	71	395	2 050	731	2 144	159	315	356	1 866
1934	950	2 688	51	101	313	1 849	659	2 311	144	341	281	1 729
1913	554	1 260	10	0	147	1 134	480	1 137	7	1	89	1 018
1933	393	726	6	0	124	585	285	642	46	8	85	531
1934	440	591	26	1	88	431	338	494	68	5	54	335

"Statistischen Jahrbuchs fuer das deutsche Reich" Jahrgang 1935 (фрагмент)
(стр. 195, 7 строка таблицы, 5 колонка –. подчёркнуты ключевые гаммы)

Место справочника, с которого начиналась выборка очередной гаммы, обозначалось пятизначной группой и добавлялось в текст шифрограммы. Первые три цифры являлись номером страницы, следующая цифра обозначала строку в таблице на этой странице, а последняя цифра – номер колонки на странице, где располагались нужные цифры (без учёта первого столбца).

Например, пусть разведчики начинали выборку гаммы с 193 страницы седьмой строки пятого столбца. Обозначалось это как 19375. Для еще большей надежности они никогда не брали первые цифры, а всегда начинали шифрование с последнего знака соответствующей колонки. Но в таком виде ключевая группа не оставлялась, а проходила определенную обработку. Для этого к ней опять же по модулю 10 прибавлялась четвертая «пятерка» с начала и третья «пятерка» с конца каждой новой шифровки. Получившуюся сумму помещали в начале криптограммы, как индикатор к расшифровке всего текста.

Здесь:

01853 – четвертая группа от начала криптограммы.
+ 26093 – третья группа от конца криптограммы.
+ 19375 – страница/строка/колонка.
36111 – ключевая группа – индикатор.

Отдельно следует объяснить, как шла передача цифрового текста. Числа выделялись в шифрограммах разделителем 94 с двух сторон, а сами цифры писались сдвоенными. Например:

WHOCOMMANDS / 5 3 / ARMY
91 98 2 80 2 96 96 5 7 83 0 94 55 33 94 5 4 96 97
(Кто командует 53 армией?)

Перехват радиосообщений Зорге велся японской полицией в течение нескольких лет, колонки загадочных пятизначных групп аккуратно подшивались в досье не пойманных шпионов. Но до самого конца японские эксперты не смогли прочесть не единой их шифрограммы. И только арестованный радист группы Макс Клаузен осенью 1941 года прояснил контрразведке систему своего шифра. Не вдаваясь в причины этого прискорбного факта, акцентируем внимание на другом – времени его появления в арсенале разведчиков.

Зорге прибыл в Японию с секретной миссией в 1933 году, но совершенно ясно, что тогда он имел

совершенно иной ключ к шифру. Ведь его статистический справочник был датирован 1935 годом! Но как раз летом 1935 года резидент выехал в Москву для кратковременного отдыха, консультаций и решения практических задач, стоящих перед его разведгруппой. Нет сомнения, что именно в этот момент ГРУ и снабдило его новой системой шифра, которая в течение следующих долгих шести лет надежно защищала наших разведчиков от упорных поисков контрразведкой Японии.

Всё вроде бы теперь ясно, но есть некоторая загадка шифра Рамзая, о которой нужно сказать. В огромной литературе о советском разведчике, изданной за рубежом и в СССР, часто присутствует мысль, что шифр Зорге привязывался еще и к дате посланного сообщения. Например, такой известный советский биограф Зорге, как Юрий Корольков в своей книге «Кио ку мицу!» писал:

«Зорге достал с полки изрядно потрепанный статистический справочник по Германии - "Ярбух - 1935 год", взглянул на календарь: 14 сентября 1941 года, перелистал, нашел нужную страницу. Старый справочник продолжал служить Зорге верой и правдой. Это был ключ к шифрованным передачам, совершенно оригинальный и безотказный, каждый раз новый и поэтому не раскрываемый… Нужно было только раскрыть страницу, соответствующую числу календаря. Дальнейшая зашифровка не составляла значительного труда».

Другие источники сообщают, что связь между номером страницы шифровальной книги и датой сообщения определялась при помощи обычных календарей. И обнаружение этих календарей при арестах членов группы с пометками арестованных, позволило японским криптологам разобрать шифр разведчиков.

Все эти домыслы имеют мало общего с действительной конструкцией шифра и историческими фактами, которые ныне обнародованы. Более того, немецким историком Юлиусом Мадером ещё в 1966 году в книге «Доктор Зорге радирует из Токио» опубликованы воспоминания оставшегося в живых радиста группы Макса Клаузена, где он подробно дает объяснения к своему шифру. В них версия Ю.Королькова никак не подтверждается! Однако в СССР была издана ещё одна книга, реально дающая ответ на заданный нами вопрос. Речь идет о широко известном в свое время романе Евгения Воробьева «Этьен и его тень» («Земля, до востребования») о знаменитом советском разведчике Льве Маневиче, работающем в предвоенные годы в Италии. Рассказывая читателю о шифре Этьена (Маневича), писатель явно списал его с группы Зорге (ссылаясь при этом того же Макса Клаузена!). Вот нужная цитата:

«Совет Клаузена … оказался весьма полезным: после каждой радиопередачи, какой бы короткой она ни была, «Травиата» меняла код. При таком условии Этьен мог быть уверен, что итальянские дешифровщики будут сбиты с толку, им никак не найти ключ от шифра, даже если они снова обнаружат «Травиату» в эфире.

Радиокод представляет систему чисел, которые перестраиваются в определенном порядке, в зависимости от дня недели.

Шифр, которым пользовалась Ингрид (радистка Этьена – А.С.), опирался на слово «Бенито». Каждая из этих шести букв несла свою цифровую нагрузку и своеобразно переводила на язык цифр весь алфавит.

У Ингрид и у Фридриха Великого, работавшего на радиосвязи в Швейцарии, был под рукой один и тот же международный статистический справочник, битком набитый цифирью.

Милан и Лозанна заранее уславливались, с какой страницы, с какой строчки и с какой буквы в слове начнут они свои очередные вычисления. А потом уже следовало помнить, на какой цифре окончится последний разговор, и с какого слова начнется новая радиограмма, по новому коду, обусловленному тем или другим днем недели».

Мысль о том, что ключ Зорге «SUBWAY» мог трансформироваться в зависимости от определенного дня недели, ежедневно меняя всю базовую шифротаблицу разведчиков, является весьма правдоподобной. Это простое решение значительно добавляло стойкости шифру Рамзая. Но если всё так, то никакие подробности, как это делалось, более автору неизвестны.

Понедельник	M	T	T

Интересно рассказать здесь и о том, как в телеграммах шло согласование времени выхода разведчиков в эфир. Для этого они пользовались словами из немецкой пословицы: «Morgenstunde hat Gold im Munde». Их записывали против дней недели в

Вторник	O	U	G
Среда	R	N	O
Четверг	G	D	L
Пятница	E	E	D
Суббота	N	H	i
Воскресенье	S	A	M

три столбика. Сочетание букв обозначало день недели.

Например, сочетание NHI указывало субботу. Допустим, передавали код: NHI30. Тогда надо было взять дату ближайшей пятницы – допустим, это было 12-е число, отнять ее от переданного числа и получить время передачи. В нашем случае 18 часов.

Кроме того, для основных географических названий и персонажей, упоминавшихся в радиограммах в Центр, использовались специальные кодовые имена, которые периодически менялись. Всё это вместе взятое не оставляло японским экспертам никаких шансов самостоятельно проникнуть в тайну шифрограмм группы Рамзая. И причины её провала осенью 1941 года до сих пор являются темой размышлений для многочисленных писателей и историков. Здесь присутствует и косвенная связь с компартией, и возможная пеленгация радиопередатчика, и постоянные вынужденные нарушения правил конспирации членами организации в условиях жесточайшего цейтнота – фашистские армии вовсю рвались к Москве. Шансов на спасение не было. Оставалось выполнять свой долг, и он был исполнен до конца!

С 1938 года Зорге получил разрешение Центра на привлечение к зашифровке радиограмм своего радиста, что в тех условиях было совершенно необходимой мерой. Макс Клаузен являлся специалистом высочайшей квалификации, изобретательности и образцом преданности делу. Поражает скорость, с которой он был способен зашифровывать свои телеграммы – 500 групп в час! Только с середины 1939 года по день ареста М. Клаузен передал в эфир сто шесть тысяч групп цифрового текста, свыше двух тысяч радиограмм, то есть в среднем - шестьсот радиограмм в год или по две радиограммы в день. Более интенсивного радиообмена в условиях конспирации трудно себе представить.

При всё нарастающем потоке информации из Токио, предположить, что сам Зорге был способен заниматься сложнейшим долгим и монотонным делом зашифровки телеграмм просто невозможно! И если мы рассмотрим деятельность других резидентур советской разведки (например, Шандора Радо или Леопольда Треппера), то увидим везде в них наличие для этой цели специальных сотрудников. Вынужденной ошибкой Зорге было объединение в одном лице функций радиста и шифровальщика, но у него, значит, не было другого выхода. Япония – не Европа, где кадровая проблема решалась в разведке значительно проще.

Интересно, поделились ли японцы со своими германскими коллегами сведениями о захваченном ими шифре ГРУ? Ведь принципы его были повторены и в шифропереписке той же «Красной капеллы», радиомузыка которой вводила в бешенство опытнейших фашистских контрразведчиков. Но это уже следующая история.

Здесь читайте:

"Лица в штатском" (биографический указатель).

Проект ХРОНОС существует с 20 января 2000 года,

на следующих доменах:
www.hrono.ru
www.hrono.info
www.hronos.km.ru,

Редактор Вячеслав Румянцев

Андрей Синельников

ШИФРЫ СОВЕТСКОЙ РАЗВЕДКИ

Шифры тоже сражались!

26 июня 1941 года, через четыре дня после начала Великой Отечественной Войны, когда над небольшой деревушкой Кранц в Восточной Пруссии только светало, сонный радист абверовской пеленгаторной установки услышал сигналы, принадлежность которых он не сумел определить. Ему были знакомы позывные всех шпионских радиостанций Европы, однако этот передатчик, несколько раз повторивший код «РТХ», он слышал впервые. Радист продолжал слушать.

Около трех часов пятидесяти минут утра неизвестная рация выстрелила в эфир радиограмму. **«KLK из РТХ 2606 0330 32WES N14KBV**…

- записал оператор, затем последовали тридцать две пятизначные группы цифр, заканчивавшихся подписью **«AR 50 385 KLK из РТХ…»**.

Несколько дней подряд спецы из абвера следили за «РТХ», однако так ничего и не смогли понять, кроме того, что передающая станция находится где-то к юго-западу от германо-советской границы. Но вскоре абверовские специалисты сделали важное открытие: кто-то отвечал «РТХ». Местонахождение этой станции не вызывало сомнений: где-то рядом с Москвой. Через несколько дней в эфире заработал другой радиопередатчик, передающий такие же пятизначные группы сигналов. И ему также ответила станция, расположенная под Москвой. Всем радиопостам в Южной Германии было приказано держать пеленг. В результате было установлено, что одна из станций с позывными «РТХ» находится в Брюсселе, а другая – в Париже.

Леопольд Треппер

В последующие две недели в эфир один за другим выходили новые передатчики (в том числе и в самом Берлине!), использующие те же самые пятизначные группы чисел. И всем им отвечала Москва. В абвере все эти станции окрестили «Die Rote Kapelle», что в переводе означает «Красная капелла». В июле 1941 года на Москву заработали также три радиопередатчика из нейтральной Швейцарии. Им, в свою очередь, присвоили название «Красной тройки». Известие об обнаруженной широкой советской шпионской сети быстро достигло ушей главы абвера адмирала Канариса. Его соперник Гейдрих, возглавлявший службу безопасности Третьего рейха, также узнал об этом. А через несколько дней о красных «музыкантах» знал уже и сам Гитлер. Фюрер был разгневан, особенно тем фактом, что шпионы действуют в его собственной столице. Абверу и СД в оккупированных странах Западной Европы, так же, как и гестапо в Германии, было приказано любой ценой выйти на след неизвестных «пианистов», шифр которых оставался загадкой для лучших немецких экспертов.

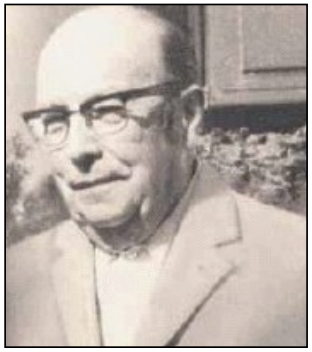
Таково начало этой великой истории, многократно под самыми разными углами описанной историками и участниками тех драматических событий, повествующей о подвиге многих и предательстве некоторых. Ценой невероятных усилий, используя все методы воздействия на пойманных разведчиков, немецкой контрразведке удалось проникнуть в тайну некоторых их радиограмм.

В декабре 1941 года была запеленгована первая радиостанция «Красного оркестра». 13 декабря отряд солдат, неслышно ступая сапогами, поверх которых были надеты носки, бесшумно поднялся на второй этаж дома 101 по улице Аттребатов в Брюсселе. Они ворвались в одну из комнат и арестовали там радиста-шифровальщика и двух других советских агентов. Чудом из рук фашистов ушел резидент Леопольд Треппер. В камине дома немцы обнаружили обугленный клочок бумаги, исписанный цифрами. Ясно, что это были записи, сделанные в процессе шифрования какого-то сообщения, и немецкие дешифровальщики немедленно принялись за его изучение. Фраза, записанная на найденном клочке бумаги, была на французском языке и больше походила на часть ключа, чем на открытый текст. В этой фразе присутствовало слово «ПРОКТОР». Служба радиоразведки допросила хозяйку, наивную пожилую вдову, которая перечислила одиннадцать книг, которые читал ее постоялец. На 286-й странице научно-фантастического романа французского писателя Ги де Терамона «Чудо профессора Вальмара» дешифровальщики нашли действующее лицо с именем Проктор. Они сумели правильно понять важность

этого совпадения. Роман Терамона дал им возможность прочесть 120 шифровок, которые принадлежали одной из самых активных радиостанций «Красной капеллы». В разобранных сообщениях говорилось о весеннем наступлении немцев на Кавказе, давались данные о состоянии немецких ВВС, приводились сведения о потреблении горючего, о потерях и содержалась некоторая другая важная информация. И главное – в одной из своих радиограмм в Брюссель Москва прямо назвала берлинские адреса советских агентов! Это был прямой путь к их гибели. Фашистские контрразведчики ликовали! А служба радиоперехвата в поисках остальных вражеских раций удвоила усилия. Ведь только запеленговав станции и схватив радистов, можно было рассчитывать, что ценой пыток и предательства удастся пробиться через броню советского шифра.

Большинство их были основаны на использовании тех или иных книг и это общеизвестно. Так, например, вторым и основным шифром группы Л. Треппера являлся роман О. Бальзака «Тридцатилетняя женщина». Одним из шифров организации Ш. Радо в Швейцарии была книга Д. Лондона «Железная пята». Радистка советской резидентуры в Швеции С. Эриксон использовала для кодирования запрещенную в Германии книгу Я. Гашека «Похождения бравого солдата Швейка». Резидент ГРУ в Болгарии С. Побережник шифровал по роману Р. Киплинга «Свет погас». А советский разведчик А. Пеев в той же Болгарии кодировал свои радиограммы по книге А. Константинова «Бай Ганю». Но как строились и работали подобные шифры, сведений в нашей прессе практически не было. В СССР издавались мемуары уцелевших руководителей знаменитых разведгрупп Леопольда Треппера, Шандора Радо и Рут Кучински. Но и в них мы мало, что сможем обнаружить нового. Это и досадно, и мало понятно. Ведь в западной литературе всё это было давным давно известно и описано.

Воспользуемся поэтому книгой известного на Западе историка «Красной капеллы» Хайнца Хене «Пароль: Директор», изданной в ФРГ в1971 году и очень нелестно встреченной тем же Л. Треппером. Не вдаваясь в явный антисоветизм этого исследования, заметим, что и сам Хене, описав в ней систему одного из советских шифров, очевидно пользовался воспоминаниями Отто Пюнтера - члена швейцарской разведгруппы, известной на Западе как «Красная тройка». Журналист и владелец информационного агентства в Женеве, Пюнтер располагал широкими связями как в журналистских, так и дипломатических кругах и даже в швейцарских правительственных органах. По своим убеждениям Пюнтер был социалист левого направления и симпатизировал Советскому Союзу. Он сам согласился помогать нашей разведке из идейных побуждений, рассматривая борьбу с фашизмом своим гражданским долгом. В конце 1942 года , перед явной угрозой оккупации Швейцарии Германией, резидент ГРУ Шандор Радо получил разрешение Центра обучить шифру ближайших своих помощников, в том числе и Пюнтера, носящего кодовое имя Пакбо. С этого момента и до самого конца существования группы Пюнтер принимал самое непосредственное участие в шифровке телеграмм, которые затем уходили в Москву через подпольные передатчики.



Отто Пюнтер

Система шифра «Красной тройки» несколько отличалась от «квадратного пропорционального метода» Рихарда Зорге, позволяющего значительно «сжимать» шифруемый текст. Но суть оставалась той же. К тому же здесь с легкостью использовалась уже любая книга. Предположим, разведчик хотел сообщить в Москву, что «Лейбштандарт СС Адольф Гитлер» прибыл в Варшаву. Для кодирования своего послания Пюнтер применил путевые заметки шведского исследователя Свена Хидина «От полюса к полюсу» и выписал случайное предложение со страницы 12: «Документальные съемки приостановлены, но вскоре будут возобновлены снова». Поскольку для ключевого слова ему требовались только десять букв, он взял часть первого слова **«Dokumentar»** (по-немецки). Пюнтер записал ключевое слово прописью и ниже его в две строчки буквы алфавита, не содержащиеся в слове «Dokumentar». По левому краю трех строк он проставил свои условные цифры (**461**), а над ключевым словом выписал порядковые номера соответствующих букв в латинском алфавите. В результате каждая буква выражалась двузначным числом: A - 14, B - 26, C – 76 (первая цифра – столбец, вторая – строка в табличке).

	2	7	4	0	5	3	6	9	1	8
4	**D**	**O**	**K**	**U**	**M**	**E**	**N**	**T**	**A**	**R**
6	B	C	F	G	H	I	J	L	P	Q
1	S	V	W	X	Y	Z	.	/		

Теперь Пюнтер мог кодировать свое послание. Он сократил его до самой краткой телеграфной формы: **«Hitlerstandarte in Warschau»** (Гитлершдандарт в Варшаве), перевел это в цифры, указанные ключевым словом, и расположил группами по пять знаков. В результате получилось следующее:

56369 49634 84219 41464 24148 49434 36644 11484 21765 61404

Затем настал черед повторного шифрования. Пакбо записал все предложение: «Документальные съемки приостановлены, но вскоре будут возобновлены снова» (конечно, по немецки) и заменил его в цифрами, но по системе, отличавшейся от первоначального кодирования, которая использовала однозначные цифры для обозначения букв, а не двузначные. Вторая цифра просто опускалась. Таким образом A становилась единицей, B - двойкой, C - семеркой и т. д. В итоге получалась одноразовая псевдослучайная гамма. Наконец Пюнтер складывал числа первого и второго кодирования по модулю 10. Теперь послание было перекрыто дважды.

В конце сообщения разведчик добавлял последнюю группу, предназначенную для адресата в Москве, который, безусловно, знал, где искать в книге Свена Хидина ключевое слово. Последняя группа в послании о «Leibstandarte» была «12085», обозначавшая: «страница 12, строка 8, слово 5».

Дважды зашифрованные таким образом, советские кодированные шарады почти не поддавались разгадке. И все же у них было одно слабое место: попади в руки противника ключевое слово или даже сама книга, и вопрос расшифровки становился делом времени. Что мы и видели в случае провала радистов в Бельгии на улице Атребаты.

Между прочим, имелась прямая связь в шифрообеспечении разведгрупп Л. Треппера и Ш. Радо. Хорошо известно, что заместитель Треппера Анатолий Гуревич (Кент) по заданию Центра в 1940 году выезжал в Швейцарию для обучения Радо шифровальному делу. Следовательно, можно утверждать, что швейцарские шифры были аналогичны системам бельгийской и французской разведгрупп ГРУ, к которым непосредственное отношение имел всё тот же Кент.

Шандор Радо

Помимо системы, описанной Пюнтером, очевидно были и другие её варианты. Вот, к примеру, радиограмма, направленная в апреле 1943 года в Швейцарию для другой помощницы Радо (Альберта) Рашель Дюпендорфер (Сиси):

«23.4.43. Сиси. Сообщаем название новой книги для вашего шифра. Купите ее, и мы дадим вам правила пользования. Альберт не должен знать новой книги. Она называется «Буря над домом», издательство Эберс, 471-я страница. Директор».

Вероятно, указанная страница планировалась лишь для первой шифрограммы разведчицы, с последующим переходом на обычный способ.

Кое что о нём сообщает в своих мемуарах и Радо: «код ежедневно менялся. И если нацисты не успевали прослушать и записать первые (а ведь Пюнтер писал про последнюю группу! – А.С.) цифровые группы, которые являлись началом кода, то, даже имея в руках нужную кодовую книгу, им очень трудно было, если вообще возможно, расшифровать радиограмму». Ясно и то, что этот самый «индикатор» шифра тоже должна была каким-то образом кодироваться по аналогии с криптографической системой Рамзая.

Показателен и радиошифр Александра Фута – еще одного помощника и радиста Радо. Он оказался прямо идентичен системе токийской разведгруппы Зорге! Фут использовал тот же квадратный пропорциональный принцип преображения букв и аналогичный сборник по промышленной статистике для получения гамм. И вряд ли это случайность. Ведь подготовкой Фута в Швейцарии занималась Рут Кучински, «крестница» Зорге и Клаузена, прошедшая в середине 30-х годов интенсивное обучение в московском Центре. Конечно, шифр Рамзая был условлен еще в 1935 г., и дистанция до шифров разведгрупп Радо и Треппера к 1943 г. составляла почти 8 лет. Но система советского шифра была настолько удачна, что еще и долгие годы и после войны её составные элементы широко применялись в криптографии. Но об этом мы расскажем немного позже. А пока перенесемся за океан в Соединенные Штаты Америки, где с подачи наших разведчиков разыгрывалась еще одна драматическая история войны, под названием «Венона».

Здесь читайте:

"Лица в штатском" (биографический указатель).

Проект ХРОНОС существует с 20 января 2000 года,

на следующих доменах:
www.hrono.ru
www.hrono.info
www.hronos.km.ru,

Редактор Вячеслав Румянцев

Андрей Синельников

ШИФРЫ СОВЕТСКОЙ РАЗВЕДКИ

Там за океаном…

Советский Союз надежно обеспечивал безопасность своей дипломатической и разведывательной переписки, применяя для ее зашифрования одноразовые шифроблокноты, использующиеся уже с 1930 года. Поэтому любые планы, которые СССР мог вынашивать против тех, кто в конце войны должен был стать их противниками, так и остались бы наиболее неприкосновенными из его секретов. ...Однако вечером 5 сентября 1945 года в Оттаве бежал на Запад 26-летний шифровальщик советского посольства в Канаде Игорь Гузенко. Он передал канадцам и американцам не только списки всех известных ему советских агентов, но и систему шифровки, принятую в ГРУ и НКГБ СССР. Информация Гузенко оказалась весьма кстати. Уже в течение нескольких лет американские криптоаналитики делали безуспешные попытки проникнуть в тайну русских шифровок, которые в изобилии уходили из вашингтонского посольства в Москву. Под именем «Венона» эта секретнейшая операция американской разведки ныне известна во всех своих подробностях. Нас же здесь интересуют исключительно системы шифров советских разведчиков, которые в деталях обрисовал американцам предатель. Об этом тоже сегодня известно. Воспользуемся здесь книгой Льва Лайнера (Бориса Сыркова) ««Венона»- самая секретная операция американских спецслужб» (М., 2003), к которой более нечего прибавить. И если раньше в центре нашего внимания были агентурные шифры разведчиков, то теперь мы обратимся уже к шифрам государства.

Донесение, предназначенное для отправки в Москву, посольский шифровальщик сначала превращал в последовательность четырехзначных цифр с использованием так называемой кодовой книги. Кодовая книга представляет собой разновидность словаря, в котором каждой букве, слогу, слову или даже целой фразе сопоставляются числа. Такие же числа зарезервированы и для знаков пунктуации, и для цифр. Если слово или фраза в кодовой книге отсутствуют, то они, как правило, разбиваются на слоги или буквы, которые, в свою очередь, заменяются числами согласно кодовой книге. Для имен и географических названий, для которых в донесении в Москву необходимо было привести их точное написание с использованием латинского алфавита, была предусмотрена отдельная кодовая книга. Ее называли «таблицей произношения».

Допустим, следовало зашифровать депешу следующего содержания:

««Гном» передал отчет об истребителе».

Шифровальщик превратил текст телеграммы при помощи кодовой книги в цепочку четырехзначных чисел:

8045 3268 2240 4983 3277

Затем он перегруппировал цифры в этой последовательности, разбив их на группы по пять цифр в каждой - 80453 26822 40498 33277, а после этого взял в руки так называемый одноразовый шифроблокнот. Одноразовым он назывался потому, что для зашифрования донесения его можно было использовать только один раз. Каждая страница блокнота содержала 60 пятизначных групп. Шифровальщик выбрал первую группу, расположенную в левом верхнем углу страницы блокнота (37584), и записал ее в качестве начальной группы шифровки. Эта группа, называемая индикатором, должна была помочь его коллеге в Москве определить, какую именно страницу блокнота следовало использовать.

Далее шифровальщик выписал следующие за индикатором пятизначные группы из блокнота под группами, которые у него получились после кодирования телеграммы с помощью кодовой книги. Он сложил все пары чисел между собой слева направо, при этом если в результате сложения у него подучалось число большее 9, то 1, обозначающая десяток, отбрасывалась. В результате шифровальщик вычислил новую последовательность пятизначных групп, которые он записал сразу вслед за индикатором:

После кодирования: 80453 26822 40498 33277
Из шифроблокнота: 37584 67439 30842 46793 34809
Шифровка: 37584 47882 56664 86181 67076

На заключительном этапе, пятизначные цифровые группы были преобразованы в пятизначные буквенные группы с использованием следующей таблицы:

0	1	2	3	4	5	6	7	8	9
O	I	U	Z	T	R	E	W	A	(?)

В большинстве дипломатических шифросистем, которыми Советская Россия пользовалась во время Второй мировой войны, в качестве индикатора задействовался номер страницы шифроблокнота, применяемой для зашифрования сообщения (обычно в блокноте было либо 35, либо 50 страниц). Советская разведка придерживалась этого правила вплоть до 1 мая 1944 года, после чего вместо номера страницы стала применять пятизначную цифровую группу, с которой начиналась страница шифроблокнота.

Преобразование цифр в буквы служило, скорее всего, для того, чтобы сократить расходы на передачу шифровки в виде телеграфного сообщения. Одно время передавать по телеграфу буквы было дешевле, чем цифры. И хотя в 40-е годы, с точки зрения оплаты, было уже неважно, из букв или же из цифр состояло телеграфное сообщение, русские по-прежнему отправляли свои телеграммы в буквенном виде.

В результате получилась шифровка следующего вида:

ZWRAT TWAAU REEET AEIAI EW0WE RWWEO 12315

В конец этой шифровки была добавлена пятизначная цифровая группа, идущая в шифроблокноте за группой, которую шифровальщик использовал последней (57760 или RWWEO), а также еще пять цифр, первые три из которых обозначали порядковый номер шифровки (123), а последние два число, которым она датировалась (15).

В Москве шифровальщик преобразовал пятизначные буквенные группы полученной шифровки в пятизначные цифровые группы:

(37584)47882 56664 8618167076(57760)

Первая из этих пятизначных групп подсказала московскому шифровальщику, какую страницу одноразового шифроблокнота следует использовать, а последняя — помогла убедиться, что ни одна пятизначная группа не была пропущена при передаче донесения. Далее он по очереди вычел цифры, приведенные на соответствующей странице блокнота, из цифр шифровки (при этом, если вычитаемое оказывалось больше уменьшаемого, последнее увеличивалось на 10). Так им была вычислена исходная цифровая последовательность пятизначных групп:

80453 26822 40498 33277

После разбивки этой последовательности на группы из четырех цифр шифровальщик в Москве восстановил исходный открытый текст донесения, применив обратное преобразование в соответствии с кодовой книгой:

8045 3268 2240 4983 3277 - ««Гном» передал отчет об истребителе».

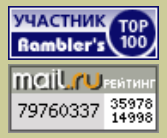
Метод двойного советского шифра был абсолютно не вскрываемым. Даже если бы американцы каким-либо образом раздобыли кодовую книгу и узнали бы в деталях об этой шифросистеме, они всё равно мало бы продвинулись в ее прочтении. Стойкость такой системы определяется, во-первых, случайностью (т. е. непредсказуемостью) последовательности знаков, из которых состоит шифроблокнот, а во-вторых, уникальностью этой последовательности. Последнее означает, что каждая страница блокнота используется для зашифрования и расшифрования донесений один и только один раз. При строгом соблюдении обоих этих условий взломать криптосистему, построенную на основе одноразового шифроблокнота, невозможно.

Однако такая абсолютная стойкость давалась очень дорогой ценой. Поскольку каждое разведывательное донесение после кодирования приходилось дополнительно шифровать с помощью уникальной цифровой цепи, для засекречивания сотен тысяч сообщений количество страниц в блокноте должно было исчисляться теми же сотнями тысяч. В 40-е годы, в отсутствие быстродействующих компьютеров, которые можно было бы использовать для автоматизации процесса создания шифроблокнотов, вручную изготовить совершенно случайную последовательность длиной несколько сот тысяч знаков оказалось просто невозможно.

Это делало применение системы одноразовых блокнотов страшно затратным и предопределило невозможность широкого использования их в военное время в стратегической агентурной разведке. Результатом этого обстоятельства и было массовое применение для получения шифровальных гамм текстов тех или иных книг. И только на уровне посольских резидентур можно было пойти на одноразовый абсолютный шифр. Однако ошибки разведчиков, многократно использующих для шифровки сведений страницы из одних и тех же шифроблокнотов (из-за невозможности обеспечить их нужное количество в Вашингтоне), привели к взлому американскими криптологами многих шифрограмм советской разведки. Что и являлось целью знаменитой операции «Венона», о которой с блеском рассказал нам писатель Лев Лайнер.

Здесь читайте:

"Лица в штатском" (биографический указатель).

	СТАТЬИ НА ИСТОРИЧЕСКИЕ ТЕМЫ
	**Проект ХРОНОС существует с 20 января 2000 года,** **на следующих доменах:** www.hrono.ru www.hrono.info www.hronos.km.ru**,** **Редактор Вячеслав Румянцев** **При цитировании давайте ссылку на ХРОНОС**

Андрей Синельников

ШИФРЫ СОВЕТСКОЙ РАЗВЕДКИ

Марк, Вик и пять центов

Жарким утром в понедельник 22 июня 1953 года Джеймс Бозарт, 13-летний продавец газет, получил сдачу от одной из своих клиенток в Бруклине. Это была монета в 25 центов и ещё пять пятицентовых монет. Позже Джеймс рассказывал: «Я шел по лестнице, и мелочь вдруг выскользнула у меня из рук. Когда я начал подбирать деньги, одна из монет распалась на две части. Я подобрал кусочки - в одном из них лежала микропленка. На ней был ряд цифр». Бозарт никогда раньше не видел подобного и немедленно похвастался находкой перед друзьями. Две его подружки были дочерьми полицейского и поделились информацией с отцом. Последний незамедлительно связался с детективами из Департамента полиции США, а те срочно созвонились с ФБР. Уже в среду 24 июня странная полая монета со всем своим содержимым от юного газетчика попадает к американским контрразведчикам, а 26 июня за неё берутся эксперты Федерального бюро расследований. Как и Джеймс, они тоже не могли сказать, что когда-либо раньше встречали похожие монеты-тайники, выполненные с таким искусством. Ну а попытка шифровальщиков разобрать помещенную на крошечной микроплёнке криптограмму из 207 пятизначных групп цифрового текста оказалась совершенно бесполезной.

Тем временем агенты ФБР просеивали через своё сито всех клиентов Джеймса, надеясь среди них обнаружить хозяина 5-ти центовой монеты. Но и здесь их ждало полное разочарование. Они ещё не знали, что эта монета уже полгода ходила по рукам американцев, и только счастливый случай занёс её в ФБР. Долгие четыре года таинственная находка не давала покоя контрразведчикам, которые сразу поняли, что имеют здесь дело с какой-то шпионской сетью. Единственное, что всё-таки удалось установить, так это то, что печатная машинка, на которой была изготовлена шифровка, иностранного производства. Так таинственно началось

это знаменитое «шпионское дело», которому посвящены сотни статей и десятки книг авторов всего мира. И только в нашей собственной стране мы до сих пор очень скупо рассказываем об этом.

Нежданная удача пришла к ФБР лишь в мае 1957 года. В американское посольство в Париже явился некто Юджин Маки и попросил для себя политического убежища. Он сообщил удивлённым дипломатам, что на самом деле является подполковником КГБ Рейно Хейханеном. И в течение четырех с половиной лет под именем Виктор находился на нелегальной работе в Америке. Теперь он следовал на «заслуженный отдых» обратно в СССР, куда его отправил американский резидент советской разведки Марк, разочаровавшийся в своем помощнике. Перебежчик не сильно вдавался в подробности своих отношений с Марком, который на поверку оказался знаменитым полковником советской разведки Рудольфом Ивановичем Абелем. Много позже мы узнаем его как Вильяма Генриховича Фишера – самого известного нелегала XX века в истории всех мировых разведок. В течении долгих лет, начиная с 1948 года, он сколачивал на территории «главного противника» (США) свою разведывательную сеть, о которой и сегодня мало, что известно. И только предательство собственного помощника поставило крест на его карьере.

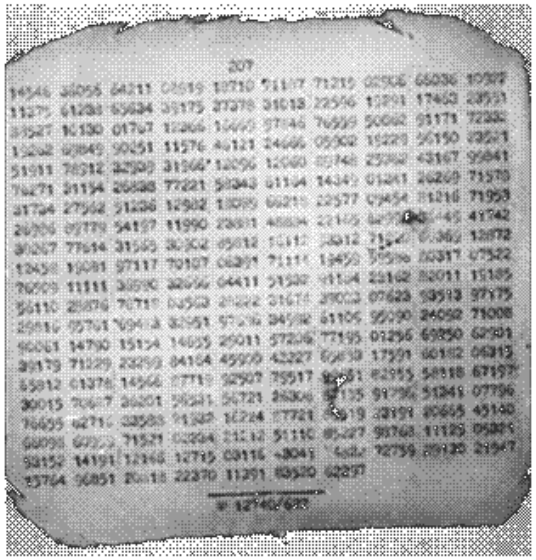
Американцы сразу же оценили всю значимость перебежчика и незамедлительно отправили его военным самолётом назад в Штаты. Здесь начались изнурительные допросы в ФБР. Хейханен сообщил, что с 1948 по 1952 год он проходил интенсивную подготовку в СССР и стажировку в Финляндии как радист-нелегал с перспективой оседания в США. Осенью 1952 года агент прибыл в Нью-Йорк, где вышел на связь с посольской резидентурой ПГУ КГБ. Летом 1954 года его передали в помощь нелегальному резиденту Марку, который особенно нуждался в хорошем помощнике-радисте. И Р. Абель конечно никак не ожидал, какой «подарок» сделает ему Москва. В течении следующих трёх лет Хейханен продемонстрировал свою полную некомпетентность как разведчик и радист, морально опускался, беспробудно пил и бил собственную супругу, тысячами воровал и растрачивал «казенные» доллары, не выполнял редкие приказы руководства и смертельно боялся возвращения на Родину. Теперь он сидел перед американскими следователями и лез «из кожи вон», чтобы стать полезным своим новым хозяевам.

Их совместными усилиями 21 июня 1957 года в отеле «Латам» Нью-Йорка наконец был арестован Абель, о работе которого в Америке Хейханен мало, что знал. Гостиничный номер Абеля и его художественная студия в Бруклине были буквально нашпигованы всевозможными «контейнерами-тайниками», специальной фото и радиоаппаратурой, наглядно подтверждающими, что сотрудники ФБР не ошиблись случайно адресом. Впрочем, это был последний их успех. Марк наотрез отказался «от сотрудничества» и контрразведчики быстро пожалели, что так поторопились с арестом русского резидента. Почти девять лет он вёл активную разведывательную работу на территории Соединённых Штатов и умудрился не оставить для ФБР никаких следов!

Приходилось надеяться на Хейханена. Помимо выдачи известных ему секретов, перебежчик в подробностях изложил сотрудникам ФБР применявшиеся им в переписке с Москвой шифросистемы и ключи к ним. Был ему задан вопрос и о злосчастной пятицентовой монете-тайнике, которая столько лет не давала покоя контрразведчикам. Предатель не ответил ничего вразумительного. Но эксперт ФБР Майкл Леонард догадался применить полученные от Хейханена сведения для чтения материала на микропленке и уже 3 июня 1957 года расшифрованный текст лежал на столе следователей. Только теперь они доподлинно убедились, что многолетние попытки специалистов вскрыть используемую здесь систему, имея на руках один только шифротекст, были абсолютно тщетными. Правда сама разобранная криптограмма сильно разочаровала американцев – шифровка предназначалась всё-таки для их вновь приобретённого агента - московский Центр поздравлял его с началом разведывательной работы и давал некоторые советы. Каким образом пять центов попали в денежный оборот Америки так и осталось не проясненным. Монета была, вероятно, обронена или истрачена часто пьяным, рассеянным Хейханеном.

Такова эта интригующая история, в которой можно найти всё – и захватывающий сюжет, и низкую измену, и беспримерное мужество со стороны её главного героя - Р.И. Абеля. 15 ноября 1957 года американский суд приговорил разведчика к 30-ти годам каторжной тюрьмы в надежде сломить русского полковника, и заставить его сотрудничать с американскими спецслужбами. Для 54-х летнего Абеля это означало

пожизненное заключение. Но всё было бесполезно. И в феврале 1962 года Абель вернулся на Родину – его обменяли на сбитого над Свердловском лётчика-шпиона Ф. Пауэрса.



К сожалению, а может быть и к счастью работа мировых спецслужб всегда покрыта непроницаемым туманом. Особо плотной завесой тайны обставлена деятельность шифровальных служб государств и их разведок – ибо нет ничего более секретного, чем их шифры. И в деле Абеля мы имеем сегодня тот редкий случай, когда можно в подробностях узнать об этих самых шифрах советских разведчиков. Причём из американских источников! Речь идёт всё о той же микроплёнке, которую с таким запозданием суждено было прочесть экспертам ФБР. Им повезло – появился деятельный предатель в лице Р. Хейханена, готовый полностью удовлетворить их любопытство. Ведь в течении длительного времени его готовили в СССР как радиста-нелегала, обучая и самым последним ухищрениям советских криптологов в области агентурных шифров. И не их вина, что многие успехи шифровальщиков свёл на нет жалкий перебежчик. Но именно через эти предательства и провалы мировые разведки узнавали с каким достойным противником они имеют дело. Не последним примером для ФБР, ЦРУ и АНБ стала и деятельность Р. Абеля. Недаром они с таким азартом и наглостью пытались перевербовать его на свою сторону. А система шифра, которую им так любезно объяснил Хейханен, просто потрясла многоопытных американских криптологов.

В отличии от обычных криптосистем Советской разведки, уже хорошо известных за период Второй мировой войны, эта (несмотря на свою некоторую схожесть) неожиданно оказалась сложнейшей системой перестановки шифруемых знаков. Исторически подобные шифры использовались мировыми разведками уже с давних пор. Но этот по праву остался вершиной среди всех известных «ручных шифров» XX века. Он был основан сразу на четырех легко запоминаемых ключах: русском слове «снегопад», патриотической дате, куплете русской песни и цифре 13. Это был личный шифр Р. Хейханена, которым пользовался только он и его руководители в Москве. И вошел он в историю западных спецслужб как шифр ВИК (VIC)– по первым буквам псевдонима Хейханена (Виктор). Но у этого красивого шифра был, разумеется, свой настоящий автор! И, очевидно, аналогичными системами пользовались в те давние времена и другие советские разведчики. Поэтому попытаемся как можно подробнее объяснить читателю этот шифр на конкретном историческом примере, встать на место наших шифровальщиков и разведчиков, попробуем увидеть всю сложность развития криптографии и заслуженно оценить искусство наших непревзойденных специалистов. Благо такую возможность дали нам сами американские эксперты, до сих

пор восхищающиеся красотой «русского шифра». Ведь еще в 1960 году (!) историк Д. Кан опубликовал в США свою статью «Номер первый из Москвы», посвящённую шифру ВИК.

Из российской энциклопедии начала XX века следует, что «несмотря на наличие самых разнообразных систем шифрования, все они основаны либо на принципе перестановки письменных знаков, либо на принципе замены одних знаков другими, либо на соединении обоих принципов вместе». Шифр ВИК середины XX века как нельзя больше соответствует этому классическому определению. Он явился причудливым конгломератом уже проверенного пропорционального шахматного шифра и последних достижений в области систем перестановок. Как было уже сказано, система основывалась одновременно на четырёх различных ключах и начиналась сложной процедурой получения многозначной псевдослучайной цифровой цепи. Генерирование таких последовательностей активно разрабатывалось в те времена криптологами всех государств для использования в качестве подстановочных гамм в типовых шифрах гаммирования. Но здесь советские специалисты пошли совсем иным путём.

Итак, разведчик для начала должен был знать на память шесть ключевых цифр (которые запоминались в форме какой-либо даты), 20 букв ключевой фразы, а также придумать пять случайных цифр, используемых в качестве индикатора сообщения.

В качестве первого ключа Хейханен использовал знаменательную дату - 3 сентября 1945 года - день победы Советского Союза над Японией, представленную цифрами: 391945.

Эта величина всегда оставалась постоянной, но для каждой конкретной криптограммы выбирался случайный пятизначный «индикатор» шифра. В данном конкретном случае было использовано число 20818.

1. Первым шагом выполнялось вычитание по модулю 10 из индикатора 20818 первых пяти цифр ключевой даты 39194 (последняя цифра 5 будет использована уже в самом конце шифрования).

```
  20818
(-) 39194
    ---------
  91724
```

2. Далее брался второй текстовой ключ. Для Хейханена московский «Центр» выбрал слова из песни М. Исаковского «Одинокая гармонь»:

Снова замерло всё до рассвета -
Дверь не скрипнет, не вспыхнет огонь.
Только слышно - на улице где-то
Одинокая бродит гармонь.

Написанное в 1945 г., это произведение поэта пользовалось огромной популярностью у всех поколений советских людей. Ключевая 20-ти буквенная фраза «Только слышно на улице г» делилась ровно на две половины. Буквы в каждой группе пронумеровывались отдельно по месту нахождения их в русской азбуке. В нашем случае нужные нам две группы букв будут выглядеть так:

Т	**О**	**Л**	**Ь**	**К**	**О**	**С**	**Л**	**Ы**	**Ш**	Н	О	Н	А	У	Л	И	Ц	Е	Г
7	**4**	**2**	**0**	**1**	**5**	**6**	**3**	**9**	**8**	6	8	7	1	9	5	4	0	3	2

3. Следующим действием была так называемая цепь дополнений, превращающая нашу, полученную в п.1, цифровую группу 91724 в десятизначную. Для этого, суммировались две рядом стоящие цифры, а результат сложения выписывался далее (подобный метод применялся в этом шифре на постоянной основе).

Здесь: 91724. Тогда: 9+1=0, 1+7=8, 7+2=9, 2+4=6, 4+0=4.

В результате получалась десятизначная последовательность: 9172408964.

4. Далее производилось суммирование цифр (опять по модулю 10), соответствующих ключевым буквам ТОЛЬКОСЛЫШ, с вновь полученной группой

```
  7 4 2 0 1 5 6 3 9 8
(+) 9 1 7 2 4 0 8 9 6 4
  ----------------------
  6 5 9 2 5 5 4 2 5 2
```

5.Следующим шагом брали вторую ключевую 10-ти буквенную группу НОНАУЛИЦЕГ и преображали соответствующие ей цифры следующим очевидным способом (верхняя строка подстановки соответствует порядковым номерам нижних знаков):

```
1 2 3 4 5 6 7 8 9 0
6 8 7 1 9 5 4 0 3 2
```

6.Используя эту перекодировку, вновь трансформировали полученную в п.4 группу цифр:

```
6 5 9 2 5 5 4 2 5 2
5 9 3 8 9 9 1 8 9 8
```

7. Последние десять цифр и являлись конечным результатом, с помощью которого, используя вновь метод цепи дополнений (см. п.3), генерировались 50 псевдослучайных цифр, необходимых в дальнейшем использовании шифра.

5	9	3	8	9	9	1	8	9	8
4	2	1	7	8	0	9	7	7	2
6	3	8	5	8	9	6	4	9	8
9	1	3	3	7	5	0	3	7	7
0	4	6	0	2	5	3	0	4	7
4	**0**	**6**	**2**	**7**	**8**	**3**	**4**	**1**	**1**

8. Заключительные 10 цифр таблицы применялись для получения другого ряда цифр, нужного для построения уже хорошо знакомого нам квадратного (шахматного) шифра. Для этого выписывали следующую табличку:

```
4 0 6 2 7 8 3 4 1 1
--------------------
5 0 7 3 8 9 4 6 1 2
```

Здесь нижняя строка есть порядковые номера цифр из верхней. Они то уже и использовались в

окончательной подстановке.

Квадратный шифр Хейханена основывался на слове «СНЕГОПАД» и имел следующий вид:

	5	**0**	**7**	**3**	**8**	**9**	**4**	**6**	**1**	**2**
	С	**Н**	**Е**	**Г**	**О**	**П**	**А**			
6	Б	Ж	**.**	К	№	Р	Ф	Ч	Ы	Ю
1	В	З	**,**	Л	н/ц	Т	Х	Ш	Ь	Я
2	Д	И	п/л	М	н/т	У	Ц	Щ	Э	пвт

Первые 7 букв ключевого слова проставлялись в верхней строке, а остальные 23 буквы и необходимые предупредительные знаки выписывались в вертикальной последовательности русского алфавита.

По сравнению с уже известными нам шифрами советских разведчиков этот имел свои особенности. Во первых, Хйханен и его руководители безбоязненно использовали здесь русскоязычный ключ в полной уверенности в бесперспективности взлома этого шифра. А ведь его возможная дешифровка в ФБР однозначно указала бы на советскую разведку, ведущую враждебную деятельность на территории США. Что и произошло впоследствии. Вспомним в этой связи предвоенные годы, когда разведчики всячески скрывали свою связь с СССР. Далее. Есть особенности и в самом построении таблички. Наиболее встречаемые в русском языке буквы можно представить в виде анаграммы «СЕНОВАЛИТР». Как видим ряд букв ключа «СНЕГОПАД» не входит в их состав. Но это не имело здесь принципиального значения, так как перед авторами шифра и не ставилась задача максимального «уплотнения» криптограмм.

Кроме того, в таблицу добавлены некоторые условные обозначения: «точка» (67), «запятая» (17), П/Л (27 - переход на латинскую азбуку), № (68 – порядковый номер), Н/Ц (18 - начало цифрового текста), «Н/Т» (28 – начало шифруемого текста), ПВТ (22 – повторение предыдущего текста). Для упрощения запоминания ключевой таблицы почти все эти обозначения соответствуют двум первым гласным буквам ключевого слова.

9. Пункты 1 – 8 являлись чисто подготовительными. Все перечисленные сложные вычисления требовались разведчикам исключительно для построения таблички преображения букв и получения цифровой последовательности, нужной для операции двойной перестановки зашифрованного текста. Причём, они использовали здесь четыре разных, но постоянных ключа. И только введение в вычисления каждый раз нового пятизначного «индикатора» позволяло полностью и до не узнаваемости менять ключи к различным криптограммам.

На первый взгляд ряд этих операций выглядят излишним усложнением шифра. Но если учесть опасность проникновения вражеской контрразведки в его систему, то эти предосторожности уже не кажутся излишними. Кроме того, так достигалась максимальная «случайность знаков» в получаемой ключевой цифровой последовательности.

Теперь мы имеем всё, чтобы самим приступить к зашифровке конкретного текста. Но для этого немного открутим историческую плёнку и вернёмся в осень 1952 года, когда новоявленный агент КГБ Рейно Хейханен оказался в Нью-Йорке. В ноябре этого года он доложил в Московский Центр (через указанные ему заранее тайники) о своей легализации в США и стал ждать указаний. В Москве в его адрес было составлено следующее письмо (орфография подлинника сохранена):

1. Поздравляем с благополучным прибытием. Подтверждаем получение вашего письма в адрес «В» повторяю «В» и прочтение письма N1.
2. Для организации прикрытия мы дали указание передать вам три тысячи местных. Перед тем как их вложить в какое либо дело посоветуйтесь с нами, сообщив характеристику этого дела.

3. По вашей просьбе рецептуру изготовления мягкой пленки и новостей передадим отдельно вместе с письмом матери.
4. Гаммы высылать вам рано. Короткие письма шифруйте, а побольше — делайте со вставками. Все данные о себе, место работы, адрес и т.д. в одной шифровке передавать нельзя. Вставки передавайте отдельно.
5. Посылку жене передали лично. С семьей все благополучно. Желаем успеха. Привет от товарищей.
N1/03 Декабря.

Воспользовавшись таблицей по ключу «СНЕГОПАД» переведём этот текст в цифрообозначения:

9 п	69 р	20 и	63 к	69 р	61 ы	19 т	20 и	12 я	23 м	61 ы	25 д	4 а	13 л
20 и	29 у	63 к	4 а	10 з	4 а	0 н	20 и	7 е	9 п	7 е	69 р	7 е	25 д
4 а	19 т	11 ь	15 в	4 а	23 м	19 т	69 р	20 и	19 т	61 ы	5 с	12 я	66 ч
20 и	23 м	7 е	5 с	19 т	0 н	61 ы	14 х	67 .	9 п	7 е	69 р	7 е	25 д
19 т	7 е	23 м	63 к	4 а	63 к	20 и	14 х	15 в	13 л	8 о	60 ж	20 и	19 т
11 ь	15 в	63 к	4 а	63 к	8 о	7 е	13 л	20 и	65 б	8 о	25 д	7 Е	13 л
8 о	9 п	8 о	5 с	8 о	15 в	7 е	19 т	29 у	20 и	19 т	7 е	5 с	11 ь
5 с	0 н	4 а	23 м	20 и	17 ,	5 с	8 о	8 о	65 б	26 щ	20 и	15 в	14 х
4 а	69 р	4 а	63 к	19 т	7 е	69 р	20 и	5 с	19 т	20 и	63 к	29 у	21 э
19 т	8 о	3 г	8 о	25 д	7 е	13 л	4 а	67 .	18 н/ц	333 333	18 н/ц	67 .	9 п

8 о	15 в	4 а	16 ш	7 е	20 и	9 п	69 р	8 о	5 с	11 ь	65 б	7 е	69 р
7 е	24 ц	7 е	9 п	19 т	29 у	69 Р	29 у	20 и	10 з	3 г	8 о	19 т	8 о
15 в	13 л	7 е	0 н	20 и	12 я	23 м	12 я	3 г	63 к	8 о	20 и	9 п	13 л
7 е	0 н	63 к	20 и	20 и	0 н	8 о	15 в	8 о	5 с	19 т	7 е	20 и	9 п
7 е	69 р	7 е	25 д	4 а	25 д	20 и	23 м	8 о	19 т	25 д	7 е	13 л	11 ь
0 н	8 о	15 в	23 м	7 е	5 с	19 т	7 е	5 с	9 п	20 и	5 с	11 ь	23 м
8 о	23 м	23 м	4 а	19 т	7 е	69 р	20 и	67 .	18 н/ц	444 444	18 н/ц	67 .	3 г
4 а	23 м	23 м	61 ы	15 в	61 ы	5 с	61 ы	13 л	4 а	19 т	11 ь	15 в	4 а
23 м	69 р	4 а	0 н	8 О	67 .	63 к	8 о	19 р	8 о	19 т	63 к	20 и	7 е
9 п	20 и	5 с	11 ь	23 м	4 а	16 ш	20 и	64 ф	69 р	29 у	20 и	19 т	7 е
17 ,	4 а	9 п	8 о	65 б	8 о	13 л	11 ь	16 ш	7 е	19 т	20 и	69 р	7 е
25 д	7 е	13 л	4 а	20 и	19 т	7 е	5 с	8 о	15 в	5 с	19 т	4 а	15 в

63 к	4 а	23 м	20 и	67 .	15 в	5 с	7 е	25 д	4 а	0 н	0 н	61 ы	7 е
8 о	5 с	7 е	65 б	7 Е	17 ,	23 м	7 е	5 с	19 т	8 о	69 р	4 а	65 б
8 о	19 т	61 ы	17 ,	4 а	25 д	69 р	7 е	5 с	20 и	19 т	67 .	25 д	67 .
15 в	8 о	25 д	0 н	8 о	20 и	16 ш	20 и	64 ф	69 р	8 о	15 в	63 к	7 е
9 п	7 е	69 р	7 е	25 д	4 а	15 в	4 а	19 т	11 ь	0 н	7 е	13 Л	11 ь
10 з	12 я	67 .	15 в	5 с	19 т	4 а	15 в	63 к	20 и	9 п	7 Е	69 р	7 е
25 д	4 а	15 в	4 а	20 и	19 т	7 е	8 о	19 т	25 д	7 е	13 л	11 ь	0 н
8 о	67 .	18 н/ц	555 555	18 н/ц	67 .	9 п	8 о	5 с	61 ы	13 л	63 к	29 у	60 ж
7 е	0 н	7 е	9 п	7 е	69 р	7 е	25 д	4 а	13 л	20 и	13 л	20 и	66 ч
0 н	8 о	67 .	5 с	5 с	7 е	23 м	11 ь	7 е	20 и	15 в	5 с	7 е	65 б
13 л	4 а	3 г	8 о	9 п	8 о	13 л	29 у	66 ч	0 н	8 о	67 .	60 ж	7 е
13 л	4 а	7 е	23 м	29 у	5 с	9 п	7 е	14 х	4 а	67 .	9 п	69 р	20 и

15 в	7 е	19 т	8 о	19 т	19 т	8 о	15 в	4 а	69 р	20 и	26 щ	7 е	20 и
68 №	18 н/ц	111 111	18 н/ц	25 д	69 р	8 о	65 б	11 ь	8 0	18 н/ц	333 333	18 н/ц	25 д
7 е	63 к	4 а	65 б	69 р	12 я	**28 н/т**	18 н/ц	111 111	18 н/ц	67 .	9 п	8 о	10 з
25 д	69 р	4 а	15 в	13 л	12 я	7 е	23 м	5 с	65 б	13 л	4 а	3 г	8 о
9 п	8 о	13 л	29 у	66 ч	0 н	61 ы	23 м	9 п	69 р	20 и	65 б	61 ы	19 т
20 и	7 е	23 м	67 .	9 п	8 о	25 д	19 т	15 в	7 е	69 р	60 ж	25 д	4 а
7 е	23 м	9 п	8 о	13 л	29 у	66 ч	7 е	0 н	20 и	7 е	15 в	4 а	16 ш
7 е	3 г	8 о	9 п	20 и	5 с	11 ь	23 м	4 а	15 в	4 а	25 д	69 р	7 е
5 с	17 ,	17 ,	15 в	22 пвт	15 в	17 ,	17 ,	20 и	9 п	69 р	8 о	66 ч	19 т
7 е	0 н	20 и	7 е	9 п	20 и	5 с	11 ь	23 м	4 а	68 №	18 н/ц	111 111	18 н/ц
67 .	18 н/ц	222 222	18 н/ц	67 .	25 д	13 л	12 я	8 о	69 р	3 г	4 а	0 н	20 и
10 з	4 а	24 ц	20 и	20 и	2	1	4						

Обратим внимание на следующие особенности этой таблицы. Зашифровка текста началась случайным образом со слова «прикрытия». А само начало сообщения через условный код Н/Т (28) вставлено в его конец. Это еще более усиливало криптозащиту документа. Интересна здесь система обозначения чисел. Каждой

цифре соответствовало их тройное повторение, что немного выпадает из ранее рассмотренных правил составления шифров советскими разведчиками. Кроме того, учитывая, что дальнейший текст нам предстоит разбить на 5-ти значные цифровые группы, в конце добавлены три цифры-пустышки для округления общего числа цифр, входящих в криптограмму

10. Основной секрет системы ВИК заключался в использовании при шифровке сложной двойной перестановки. Для этого у агента был еще небольшой личный номер - 13. Это число использовалось для определения размеров двух перестановочных таблиц (их ширины и глубины). Из 50-ти значной гаммы (см. п.7) брались две последние неравные цифры (у нас: 4 и 1), которые поочередно суммировались с личным номером. Для первой таблицы 13+4=17 столбцов, и 13+1=14 столбцов для второй перестановочной таблицы. Кроме ширины столбцов нам нужно знать ключевой набор цифр. Он извлекался из полученной ранее 50-значной последовательности. Приведем её ещё раз, добавив во вторую строку порядковые номера ключевых цифр:

5	9	3	8	9	9	1	8	9	8
3	**7**	**2**	**4**	**8**	**9**	**1**	**5**	**0**	**6**
4	2	1	7	8	0	9	7	7	2
6	3	8	5	8	9	6	4	9	8
9	1	3	3	7	5	0	3	7	7
0	4	6	0	2	5	3	0	4	7
4	0	6	2	7	8	3	4	1	1

Для двух перестановочных таблиц нам нужна в сумме 31 цифра (17+14), которые мы и выпишем поочередно вертикально из таблички согласно верхней её нумерации: 9 6 0 3 3 1 8 3 6 6 4 6 9 0 4 7 5 3 0 2 7 4 3 0 4 2 8 7 7 1 2

Стоит здесь объяснить, зачем разведчики получали в табличке 50 знаков. У Хейханена личным номером было число 13. Максимально возможная цифра, которую можно прибавить к 13 есть 9. В сумме это 22. Для двух таблиц – не более 43 знаков. Так что для Вика было важно иметь в качестве ключа именно 50 цифр.

Отметим попутно и следующий факт. В 1956 году Хейханену несколько изменили шифровальный ключ и его личным номером стало число 20. Соответственно у него должна была удлиниться и генерируемая последовательность цифр до 60 знаков. Впрочем, до измены агента оставались считанные месяцы, и предосторожности руководителей Вика были уже излишние.

Итак, для первой перестановки используем первые 17 цифр: **9 6 0 3 3 1 8 3 6 6 4 6 9 0 4 7 5**. Выписываем в нашу 17-колонную таблицу построчно весь зашифрованный в п.8 текст (во второй строке таблицы мы видим соответственно порядковые номера ключевых цифр):

9	***6***	***0***	***3***	***3***	***1***	***8***	***3***	***6***	***6***	***4***	***6***	***9***	***0***	***4***	***7***	***5***
14	***8***	***16***	***2***	***3***	***1***	***13***	***4***	***9***	***10***	***5***	***11***	***15***	***17***	***6***	***12***	***7***
9	6	9	2	0	6	3	6	9	6	1	1	9	2	0	1	2
2	3	6	1	2	5	4	1	3	2	0	2	9	6	3	4	1
0	4	0	2	0	7	9	7	6	9	7	2	5	4	1	9	1

1	1	5	4	2	3	1	9	6	9	2	0	1	9	6	1	5	
1	2	6	6	2	0	2	3	7	5	1	9	0	6	1	1	4	
6	7	9	7	6	9	7	2	5	1	9	7	2	3	6	3	4	
6	3	2	0	1	4	1	5	1	3	8	6	0	2	0	1	9	
1	1	1	5	6	3	4	6	3	8	7	1	3	2	0	6	5	
8	2	5	7	1	3	8	9	8	5	8	1	5	7	1	9	2	
9	2	0	1	9	7	5	1	1	5	0	4	2	3	2	0	1	
7	5	8	8	6	5	2	6	2	0	1	5	1	4	4	6	9	
4	6	3	1	9	7	6	9	2	0	5	1	9	2	0	6	3	
2	9	2	1	1	9	8	3	8	2	5	7	1	3	4	6	7	
1	8	3	3	3	1	8	6	7	9	8	1	5	4	1	6	7	
2	0	9	6	9	8	5	1	1	6	5	7	6	9	7	2	4	
7	9	1	9	2	9	6	9	2	9	2	0	1	0	3	8	1	
9	8	1	5	1	3	7	0	2	0	1	2	2	3	1	2	3	
6	3	8	2	0	9	1	3	7	0	6	3	2	0	2	0	0	
8	1	5	8	5	1	9	7	2	0	9	7	6	9	7	2	5	
4	2	5	2	0	2	3	8	1	9	2	5	7	1	3	1	1	
0	8	1	5	2	3	7	5	1	9	7	5	9	2	0	5	1	
1	2	3	8	2	3	2	3	4	1	9	7	6	9	2	0	6	
7	1	8	4	4	4	1	8	6	7	3	4	2	3	2	3	6	
1	1	5	6	1	5	6	1	1	3	4	1	9	1	1	1	5	
4	2	3	6	9	4	0	8	6	7	6	3	8	6	9	8	1	
9	6	3	2	0	7	9	2	0	5	1	1	2	3	4	1	6	
2	0	6	4	6	9	2	9	2	0	1	9	7	1	7	4	9	
8	6	5	8	1	3	1	1	1	6	7	1	9	2	0	6	9	

7	2	5	7	1	3	4	2	0	1	9	7	5	8	1	5	5
1	9	4	1	5	6	3	4	2	3	2	0	6	7	1	5	5
7	2	5	4	0	0	6	1	7	8	5	7	6	5	7	1	7
2	3	7	5	1	9	8	6	9	4	6	5	8	1	9	6	1
1	7	4	2	5	6	9	7	5	2	0	1	9	6	7	2	5
6	7	1	5	8	2	5	0	8	2	0	1	6	2	0	6	4
6	9	8	1	5	6	3	7	9	7	6	9	7	2	5	4	1
5	4	1	9	1	1	0	7	1	3	1	1	1	0	1	2	6
7	1	5	5	1	9	4	1	5	6	3	2	0	9	7	6	9
7	2	5	4	1	5	4	2	0	1	9	7	8	1	9	2	5
7	1	3	1	1	0	8	6	7	1	8	5	5	5	1	8	6
7	9	8	5	6	1	1	3	6	3	2	9	6	0	7	0	7
9	7	6	9	7	2	5	4	1	3	2	0	1	3	2	0	6
6	0	8	6	7	5	5	7	2	3	1	1	7	2	0	1	5
5	7	6	5	1	3	4	3	8	9	8	1	3	2	9	6	6
0	8	6	7	6	0	7	1	3	4	7	2	3	2	9	5	9
7	1	4	4	6	7	9	6	9	2	0	1	5	7	1	9	8
1	9	1	9	8	1	5	4	6	9	2	0	2	6	7	2	0
6	8	1	8	1	1	1	1	8	2	5	6	9	8	6	5	1
1	8	1	8	3	3	3	1	8	2	5	7	6	3	4	6	5
6	9	1	2	2	8	1	8	1	1	1	1	8	6	7	9	8
1	0	2	5	6	9	4	1	5	1	3	1	2	7	2	3	5
6	5	1	3	4	3	8	9	8	1	3	2	9	6	6	0	6
1	2	3	9	6	9	2	0	5	6	5	1	1	9	2	0	7
2	3	6	7	9	8	2	5	1	9	1	5	7	6	9	6	0

2	5	4	7	2	3	9	8	1	3	2	9	6	6	7	0	2
0	7	1	5	4	1	6	7	3	8	9	2	0	5	1	1	2
3	4	1	5	4	2	5	6	9	7	5	1	7	1	7	1	5
2	2	1	5	1	7	1	7	2	0	9	6	9	8	6	6	1
9	7	0	2	0	7	9	2	0	5	1	1	2	3	4	6	8
1	8	1	1	1	1	8	6	7	1	8	2	2	2	1	8	6
7	2	5	1	3	1	2	8	6	9	3	4	0	2	0	1	0
4	2	4	2	0	2	0	2	1	4							

Теперь из таблицы по столбцам выпишем последовательно цифры опять же согласно верхней её нумерации и получим 206 5-ти значных групп промежуточной криптограммы:

65730 94337 57918 93912 33454 79336 09626 19501 25307 11389
39831 27711 22124 67057 18113 69528 25846 62487 14525 19541
59657 49882 53977 55521 12020 22616 19691 39210 50224 19061
15015 85111 16771 66813 26469 24410 13061 79325 69169 36190
37853 81829 12416 70771 26347 31641 18190 58767 26821 07219
87801 55852 16927 93461 17925 60061 39822 18702 55133 51295
91830 31616 00124 04173 12730 22194 70117 97051 79172 09917
64726 29717 64102 11544 95219 37741 30511 66516 99557 15416
95676 56980 15856 70225 18606 34127 31225 69809 83128 21126
06292 37794 12197 07819 88905 23574 27822 93667 51381 22871
22721 14616 02102 79589 15076 12839 68815 85113 92076 16299
51385 50029 69000 99173 75061 38422 73611 33394 29221 11693
87051 94122 09761 14517 17023 75574 13191 70751 19127 59011
21067 11215 92161 24149 11316 90666 62 820 21503 18146 55162
64262 80016 59256 93006 01166 81349 12714 85268 85671 93721
60921 43689 53044 81554 79513 14822 96519 82092 01166 18974
21279 68401 71492 87172 16657 77796 50716 16161 22032 91749
95102 03521 91561 22679 62982 79566 89671 08561 73352 96829
17607 92209 60569 21508 32391 18551 38533 65545 74181 55386
86641 11121 36411 10154 26496 32273 42349 03091 29316 31287
51622 09150 32227 68367 69665 18322

11. Для второй перестановки текста мы берем следующие 14 цифр ключевой группы, полученной нами в п.10: 3 0 2 7 4 3 0 4 2 8 7 7 1 2. Здесь мы имеем сложную неравномерную колонную перестановку (вторая строка таблицы опять соответствует порядковым номерам верхних цифр).

Количество столбцов рассчитывается из расчета общего числа цифр в тексте (1030) и ширины таблицы (14). То есть 74 строки (74x14=1036). Треугольные области, окрашенные в таблице желтым цветом, строятся следующим образом. Их левые верхние углы соответствуют порядковым номерам ключевой строки, а нижний правый угол опирается на последний столбец таблицы.

Сначала в серую область таблицы вписывался горизонтально промежуточный текст, который доходил до

края таблицы (см. п.10), а по её заполнении наступала очередь жёлтой области.

3	***0***	***2***	***7***	***4***	***3***	***0***	***4***	***2***	***8***	***7***	***7***	***1***	***2***
5	***13***	***2***	***9***	***7***	***6***	***14***	***8***	***3***	***12***	***10***	***11***	***1***	***4***
6	5	7	3	0	9	4	3	3	7	5	7	1	1
9	1	8	9	3	9	1	2	3	3	4	5	4	2
7	9	3	3	6	0	9	6	2	6	1	9	5	0
1	2	1	5	9	2	1	6	1	2	4	1	4	9
5	3	0	1	1	3	1	6	9	0	6	6	6	6
7	1	1	3	2	8	2	0	2	1	5	0	3	1
8	9	3	9	8	8	1	4	6	5	5	1	6	2
3	1	2	7	7	1	6	4	2	6	2	8	0	0
1	2	2	1	2	4	6	1	6	5	9	2	5	6
7	0	5	7	1	8	1	1	9	3	0	0	6	0
3	6	9	5	2	8	2	5	8	1	1	6	6	8
4	6	6	2	4	8	7	1	4	5	1	3	4	9
2	5	1	9	5	4	1	5	9	6	5	1	2	7
7	4	9	8	8	2	5	3	9	7	7	5	1	4
5	5	2	1	1	2	0	2	0	2	2	6	1	8
6	1	9	6	9	1	3	9	2	1	0	5	0	2
2	4	1	9	0	6	1	1	5	2	6	8	8	5
5	0	1	5	8	5	1	1	1	6	7	1	9	3
1	6	7	7	1	6	6	8	1	3	7	2	1	6
2	6	4	6	9	2	4	4	1	0	1	0	9	2
3	0	6	1	7	9	3	2	5	6	9	1	1	4
6	9	3	6	1	9	0	3	7	8	5	3	8	3

1	8	2	9	1	2	4	1	6	7	0	7	7	1
2	6	3	4	7	3	1	6	4	1	1	8	1	6
9	0	5	8	7	6	7	2	6	8	2	1	0	7
8	9	5	3	0	4	4	8	1	5	5	4	7	9
2	5	1	3	1	4	8	2	2	9	6	5	1	9
1	9	8	2	0	9	2	0	1	1	6	6	1	8
8	7	8	9	7	4	2	1	2	7	9	6	8	4
0	1	5	5	0	1	7	1	4	9	2	8	7	1
8	5	2	1	6	7	2	1	6	6	5	7	7	7
9	2	7	9	3	4	7	9	6	5	0	7	1	8
6	1	1	7	9	2	5	1	6	1	6	1	2	2
6	0	0	6	1	3	9	8	0	3	2	9	1	7
2	2	1	8	7	0	2	5	5	4	9	9	5	1
1	3	3	6	1	2	9	5	9	1	0	2	0	3
8	3	0	3	1	6	1	6	0	0	1	5	2	1
2	4	0	4	1	7	3	1	2	7	3	0	9	1
2	2	1	9	4	7	0	1	1	7	9	7	0	9
5	1	7	9	1	7	2	0	9	9	1	7	6	4
7	2	6	2	9	6	1	2	2	6	7	9	6	2
7	1	7	6	4	1	9	8	2	7	9	5	6	6
0	2	1	1	5	4	4	8	9	6	7	1	0	8
9	5	2	1	9	3	7	7	5	6	1	7	3	3
4	1	3	0	5	1	1	6	6	5	2	9	6	8
5	1	6	9	9	5	5	7	1	5	2	9	1	7
4	1	6	9	5	6	7	6	5	6	9	6	0	7

8	0	1	5	8	5	6	7	0	2	2	5	9	2
1	8	6	0	6	3	4	1	2	7	3	1	2	2
2	5	6	9	8	0	9	8	3	1	2	8	2	1
1	2	6	0	0	9	6	0	5	6	9	2	1	5
6	2	9	2	3	0	8	3	2	3	9	1	1	8
7	7	9	4	1	2	5	5	1	3	8	5	3	3
1	9	7	0	7	8	1	6	5	5	4	5	7	4
9	8	8	9	0	5	2	3	1	8	1	5	5	3
5	7	4	2	7	8	2	2	9	8	6	8	6	6
3	6	6	7	5	1	3	8	1	2	4	1	1	1
2	8	7	1	2	2	7	2	1	1	4	1	2	1
6	1	6	0	2	1	0	2	7	9	5	8	3	6
9	1	5	0	7	6	1	2	8	3	9	6	8	4
8	1	5	8	6	1	1	3	9	2	0	7	6	1
6	2	9	9	5	1	3	1	1	1	0	1	5	4
8	5	5	0	0	2	9	6	2	6	4	9	6	3
9	0	0	0	9	9	1	7	3	2	2	7	3	4
7	5	0	6	1	3	8	4	2	2	2	3	4	9
7	3	6	1	1	3	3	3	9	4	2	0	3	0
9	2	2	1	1	1	5	9	3	8	7	0	9	1
5	1	9	4	1	2	2	0	9	7	6	1	1	2
4	5	1	7	1	7	0	2	3	7	5	5	7	4
1	3	1	9	3	1	6	3	1	2	8	7	5	1
9	1	7	0	6	2	2	0	9	1	5	0	3	2
7	5	1	1	9	2	2	7	6	8	3	6	7	6

1	2	7	5	9	0	9	6	6	5	1	8	3	2
1	1	2	1	0	6	7	2						

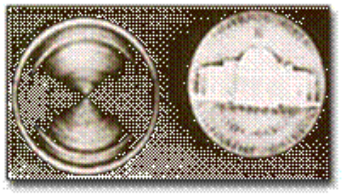
Теперь остается в последний раз выбрать цифры шифрограммы по колонкам, согласно верхней нумерации таблицы. При разбивке получаемой числовой последовательности на 5-ти значные группы мы и получим искомую шифрограмму Вика, которую и обнаружили в 5-ти центовой монете летом 1953 года.

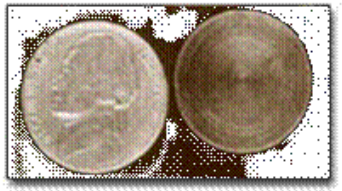
207

14546 36056 64211 08919 18710 71187 71215 02906 66036 10922
11375 61238 65634 39175 37378 31013 22596 19291 17463 23551
88527 10130 01767 12336 16669 97846 76559 50062 91171 72332
19262 69849 90251 11576 46121 24666 05902 19229 56150 23521
51911 78912 32939 31966 12096 12060 89748 25362 43167 99841
78271 31194 26838 77221 58343 61164 14349 01241 26269 71578
31734 27562 51236 12982 18089 66218 22577 09454 81216 71953
26986 89779 54197 11990 23881 48884 22165 62992 36449 41742
30267 77614 31565 30902 85812 16112 93312 71220 60369 12872
12458 19081 97117 70107 06391 71114 19459 59586 80317 07522
76509 11111 36990 32666 04411 51532 91184 23162 82011 19185
56110 28876 76718 03563 28222 31674 39023 07623 93513 97175
29816 95761 69483 32951 97686 34992 61109 95090 24092 71008
90061 14790 15154 14655 29011 57206 77195 01256 69250 62901
39179 71229 23299 84164 45900 42227 65853 17591 60182 06315
65812 01378 14566 87719 92507 79517 99651 82155 58118 67197
30015 70687 36201 56531 56721 26306 87185 91796 51341 07796
76655 62716 33588 21932 16224 87721 85519 23191 20665 45140
66098 60959 71521 02334 21212 51110 85227 98768 11125 05321
53152 14191 12166 12715 03116 43041 74822 72759 29130 21947
15764 96851 **20818** 22370 11391 83520 62297

В составленной нами криптограмме спрятан индикатор сообщения 20818 (см. п.1). Он стоит в пятой группе с конца шифра и его положение указывает последняя цифра используемой Виком в качестве ключа даты «9 сентября 1945» (см. п.1).

А в начале шифрограммы проставлено количество групп в зашифрованном тексте (207). Для расшифровки текста сначала через индикатор и условные ключи определяли размеры используемых при перестановке таблиц. У нас 206 групп (за вычетом индикатора), или 1030 цифр. Следовательно, в конечной таблице должно быть 74 строки (на 14 колонок), а в промежуточной – 61 строка (на 17 колонок). Далее требовалось только терпение и внимательность, чего явно недоставало такому шпиону, как Вик.





Любопытно, что Хейханен на судебном процессе по делу Абеля дал присяжным пространные объяснения по системе своего шифра. Но адвокат Абеля Джеймс Донован ничего в нём не понял и написал в своей книге «Незнакомцы на мосту», что «он недоступен пониманию». Несмотря на свою несомненную надежность, шифр ВИК был сложен в применении, возможны были в нем и обычные человеческие ошибки, делающие его результат абсолютно нечитаемым. Неудобно и долго было составлять с помощью подобного шифра большие криптограммы. Именно поэтому Центр советовал Вику длинные сообщения шифровать со вставками, оставляя часть текста нешифрованным, а вставки пересылать отдельно. И именно поэтому Хейханен просил у своего начальства одноразовые шифровальные блокноты (гаммы). Но в этом Вику было отказано. За пять лет пребывания в США ленивый Хейханен отправил в Центр не более тридцати сообщений, а получил в ответ примерно двадцать пять. Трудно назвать такой шифрооборот интенсивным.

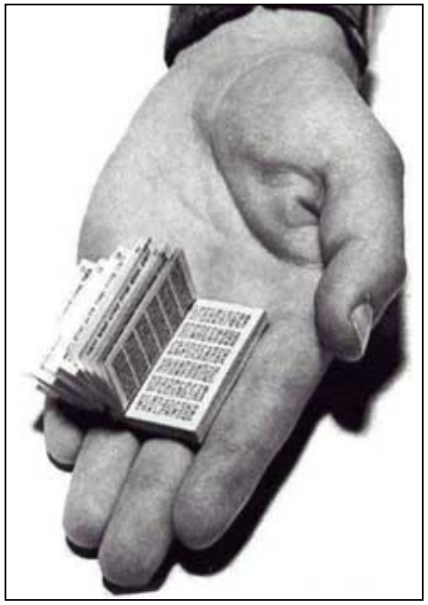
Как было уже сказано, шифр ВИК вошел в историю мировых разведок, как самый сложный из известных «ручных» систем шифрования, категорически не поддававшийся дешифровке. И эта сложность шифра лучше всего демонстрирует нам тот исключительный накал «криптологической войны», которая стала составной частью «войны холодной». Он вобрал в себя многие криптографические достижения того времени. Это и внедрение пропорционального шифра, и применение двойной неравномерной системы перестановки цифровых групп с разбивкой их на отдельные элементы, и различные мнемонические способы запоминания конструкции шифра. К этому моменту большинство советских разведчиков перешло в своей переписке с Москвой на системы одноразовых шифроблокнотов. Однако, несмотря на теоретическое совершенство, их захват вражеской контрразведкой являлся безусловной уликой в шпионской деятельности. Перестановочный шифр ВИК был свободен от этого недостатка, в то же время он мало уступал шифроблокнотам в своей криптостойкости. Но достигалось это несоразмерной ценой – исключительной трудоёмкостью подобного шифра. И совершенно понятно, что сами пользователи таких систем вряд ли были в большом от них восторге и предпочитали менее сложные способы тайнописи.

Так на вопрос американских судей о шифре самого Рудольфа Абеля Хейханен пояснил:

«Марк рассказывал мне, что … он шифровал и расшифровывал другим способом, что он пользовался специальными небольшими книжками, с помощью которых зашифровывать было значительно легче, чем с помощью этого метода».

Действительно, Рудольф Абель применял для своей переписки с Москвой одноразовые шифроблокноты. Утром 21 июня 1957 года сотрудники ФБР обнаружили один из них в комнате отеля «Латам» в Нью-Йорке в ходе обыска, последовавшего вслед за арестом Абеля. Контрразведчики осмотрели содержимое его мусорной корзины, и нашли в ней кусок дерева, к которому была прикреплена наждачная бумага. Кусок разделился на части, в нём лежал комплект из 250 шифровальных таблиц, содержавших наборы 5-ти значных цифровых групп. Они

были исполнены на тончайшей бумаге, похожей на очень тонкую серебряную фольгу. У присутствующих сложилась полная уверенность, что при необходимости разведчик мог быстро уничтожить такую бумагу, просто проглотив её без всякого ущерба для своего здоровья!



Один из шифрблокнотов советской разведки

ФБР крупно повезло – в ночь перед арестом их подопечный провёл сеанс радиосвязи с Центром. И, естественно, шифровальные принадлежности находились в номере его гостиницы. Обычно разведчик хранил их в потайном месте в городе, где, помимо шифровальных материалов, находились и другие «шпионские атрибуты». Но поскольку всё было упаковано вместе, они теперь также находились в номере.

Шифр Абеля казался довольно простым - цифры в нём просто замещали буквы сообщения. В то же время эту систему нельзя было взломать. К каждой группе чисел добавлялась случайная цифра из шифроблокнота, поэтому зашифрованное сообщение выглядело совершенно бессмысленным.

После ареста Абеля американские контрразведчики следили за его радиопередачами в соответствии с расписанием, найденным у Абеля в полом карандаше-тайнике, и дважды перехватывали радиограммы, состоявшие из пятизначных цифровых групп. Однако прочесть шифровки, даже при наличии шифроблокнота, так и не сумели. Буквально на глазах сотрудников ФБР Рудольф Иванович сумел спустить в унитаз ключ к шифру (вероятно, свою небольшую табличку преображения букв) и полученную накануне ареста шифрограмму из Москвы!

Одноразовые шифроблокноты были захвачены в те годы при аресте еще нескольких советских агентов. В начале 1961 г. в пригороде Лондона было найдено с полдюжины блокнотов в виде свернутых трубочек бумаги. Английские полицейские отыскали их в зажигалке на даче Хелен и Питера Крогер – двух советских агентов, выдававших себя за семейную американскую пару, Лону и Мориса Коэн. Остальные блокноты извлекли из другой зажигалки, обнаруженной на лондонской квартире их руководителя – советского резидента в Англии, известного под именем Гордона Лонсдейла (полковника Конона Молодого (Бена)). Наряду с шифроблокнотами английская полиция обнаружила в зажигалке Крогера и расписание радиопередач.

В соответствии с этим расписанием, настроившись на частоту 17080 килогерц, 9 января 1961 г. в 12.32 по Гринвичу полиция услышала позывной «277». Через 18 минут тот же самый позывной был принят на частоте 14755 килогерц. 18 января в 6.38 по Гринвичу на частоте 6340 килогерц снова был услышан позывной «277». Меньше чем через час этот позывной был замечен на волне 8888 килогерц. Пеленгаторы установили, что источник радиопередач находится в Москве. Лонсдейл имел высокоскоростной радиопередатчик, который посылал 240 слов в минуту. Советский разведчик записывал свои сообщения на пленку и затем на большой скорости передавал их в эфир. Между прочим, английские контрразведчики хвастались, что целых два месяца до ареста группы Бена контролировали радиопередачи разведчиков и даже дешифровали их. Но это обстоятельство весьма сомнительно.

Конон Молодый и Рудольф Абель

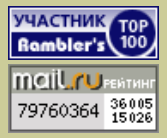
Таким образом, очевидно, что к середине XX века основным шифром советских разведчиков стали одноразовые шифроболокноты. Причем во внешнем их виде отчетливо просматривалась тенденция к уменьшению.

Так, шифроблокнот, захваченный в 1954 г., содержал 40 строк по 8 групп из 5 цифр. В другом блокноте, доступ к которому был получен в 1958 г., имелось 30 строк по 10 групп. В блокнотах, захваченных в 1957-м и 1961 гг., было 20 строк по 4 и 5 групп соответственно. Группы, строки и страницы были пронумерованы. Размножение шифроблокнотов производилось простым фотографированием, которое считалось наилучшим способом скопировать «гамму» для агента. Более того, бумага, из которой изготавливались блокноты, часто делалась из нитроклетчатки – материала, который применялся для производства фотопленки на заре кинематографа. Этот материал очень легко воспламеняется, а с помощью марганцовокислого калия, который у разведчиков всегда под рукой, обычное горение можно было превратить почти во взрыв, который быстро и полностью уничтожал шифроблокнот, не оставляя даже скрытого изображения на пепле.

Как отмечал Дэвид Кан, «советским агентам не грозит опасность быть разоблаченными из-за слабости применяемых ими шифровальных средств». Такая оценка известного историка мировой криптографии многого стоит. Неоспоримый факт: искусство советских криптологов в составлении агентурных шифров стало достоянием даже враждебных нам мировых разведок и об этом наша последняя страница.

Здесь читайте:

"Лица в штатском" (биографический указатель).

	СТАТЬИ НА ИСТОРИЧЕСКИЕ ТЕМЫ
	**Проект ХРОНОС существует с 20 января 2000 года,** **на следующих доменах:** www.hrono.ru www.hrono.info www.hronos.km.ru**,** **Редактор Вячеслав Румянцев** **При цитировании давайте ссылку на ХРОНОС**

Андрей Синельников

ШИФРЫ СОВЕТСКОЙ РАЗВЕДКИ

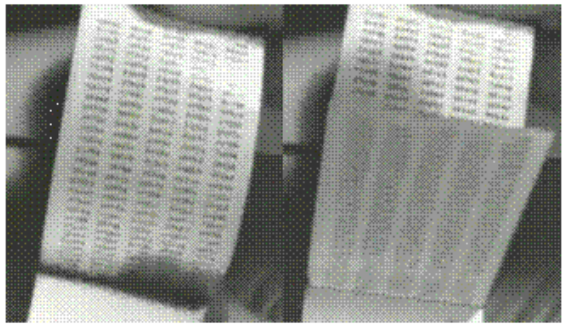
Шифры агентов ЦРУ

22 октября 1962 года в Москве был арестован полковник ГРУ, работающий под прикрытием руководящего сотрудника Государственного комитета по координации научно исследовательских работ, он же двойной агент американской и английской разведок Олег Пеньковский. В этот же день на его московской квартире сотрудники КГБ провели тщательный обыск, который дал поразительные результаты.

В письменном столе Пеньковского обнаружили хитро сделанный тайник, из которого следователь изъял шпионские принадлежности: записи Пеньковского с номерами телефонов иностранных разведчиков, шесть сигнальных открыток и инструкций к ним, донесения и экспонированные фотопленки. Здесь же были: фиктивный паспорт, шесть шифровальных блокнотов, три фотоаппарата «Минокс» и описание их, два листа копировальной бумаги для написания тайнописного текста, записка с указанием радиоволн, на которых Пеньковский принимал инструктивные радиопередачи иностранных разведок, проект донесения Пеньковского в разведцентр, пятнадцать не экспонированных фотопленок к фотоаппарату «Минокс» в кассетах и инструкции иностранных разведок по фотографированию этим фотоаппаратом, а также инструкции по шифрованию и расшифрованию радиосообщений, по процедуре приема радиопередач из разведцентра, о подборе и использовании тайников.

Были изъяты и приобщены к делу в качестве вещественных доказательств полученный Пеньковским от иностранных разведок радиоприемник «Сони», с помощью которого он принимал шифрованные радиограммы из разведцентра, и пишущая машинка, на которой шпион печатал свои донесения.

Английская и американская разведки рекомендовали Пеньковскому применять в его шпионской деятельности определенные меры предосторожности. Так, в пункте восьмом одной из инструкций говорилось: «Расклеивайте столько страниц блокнота, сколько вам нужно для зашифровки и расшифровки, но не больше. Когда страница блокнота, зашифрованная или расшифрованная, использована, сожгите ее. Храните ваши блокноты в самом безопасном месте, какое только вы можете придумать. Эти места должны быть так выбраны, чтобы ваши посещения этих мест не возбуждали ничьих подозрений. Запасные блокноты и блокноты в употреблении должны храниться в разных местах».



Провал агента был полным. И, пожалуй, нет сегодня в нашей стране более известного шпиона, чем этот самый Пеньковский. Он нанес своей Родине существенный вред. Но провалился удивительно быстро. После Пеньковского были Огородник, Толкачев, Филатов, Поташов, Нилов, Поляков… Но в этом малопочтенном тесном ряду он явился одним из первых. На нём молодые американские спецслужбы отрабатывали методы своей работы в Москве, разрабатывали способы без уликовой связи с агентами, их прикрытия и поддержки. При аресте Пеньковского была изъята гора всевозможного шпионского имущества, которую с постоянной регулярностью затем изымали и продолжают изымать наши контрразведчики у действующих американских агентов. Но вот, что интересно – все это до боли напоминает методы разведки советской, работа которой, несомненно, была наглядным уроком для ЦРУ.

Рассмотрим для примера доступные нам документы по делу Пеньковского, в частности его шифрообеспечение. Здесь мы обнаружим много интересного и знакомого. При его аресте, в частности, были изъяты:

1. Правила приема радиопередач из разведцентра.

2. Инструкция по правилам работы с шифрами и перешифровальными блокнотами.

Последняя инструкция содержала следующие наставления:

1) Правила набора открытого смыслового текста, предназначенного для зашифрования путем замены букв текста на цифровые значения и сформирование их в пятизначные группы.

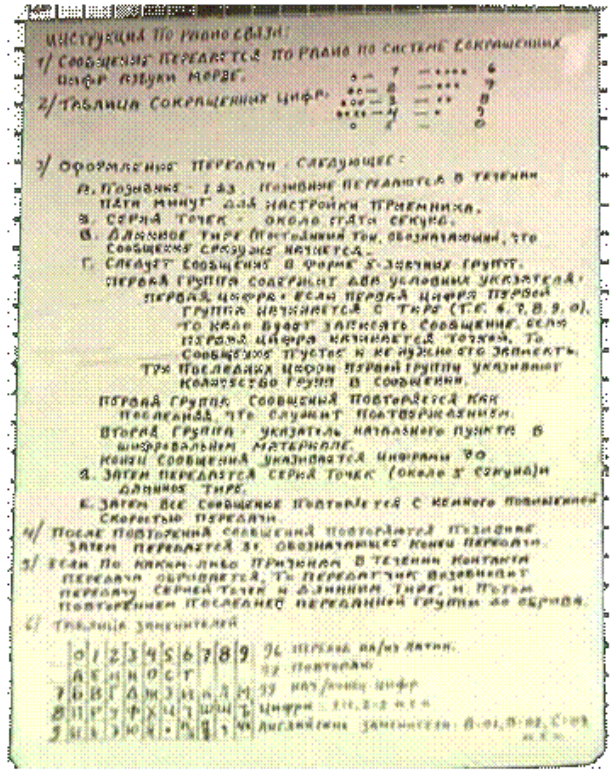
2) Порядок и правила перешифрования набранных групп способом наложения бесконечных пятизначных цифровых групп, взятых из страницы перешифровального блокнота – путем криптографического (ложного) вычитания.

Некоторые сведения об этих инструкциях можно почерпнуть из показаний самого агента:

.«1) Сообщение передается по радио по системе сокращенных цифр азбуки Морзе.

2) Таблица сокращенных цифр:

точка, тире - 1;
точка, точка, тире – 2;
точка, точка, точка, тире – 3;
точка, точка, точка, точка, тире – 4;
точка -5;
тире, точка, точка, точка, точка – 6;
тире, точка, точка, точка – 7;
тире, точка, точка – 8;
тире, точка - 9;
тире – 0.



3) Оформление передачи следующее:

А. Позывные – 163. Позывные передаются в течение пяти минут для настройки приемника.

Б. Серия точек – около пяти секунд.

В. Длинное тире – постоянный тон, обозначающий, что сообщение сразу же начнется.

Г. Следует сообщение в форме пятизначных групп. Первая группа содержит два условных указателя. Первая цифра – если первая цифра первой группы начинается с тире (т.е. 6,7,8,9,0), то надо будет записать сообщение. Если первая цифра начинается точкой, то сообщение пустое и не нужно его записывать. Три последних цифры первой группы указывают количество групп в сообщении. Первая группа сообщения повторяется как последняя, что служит подтверждением.

Вторая группа – указатель начального пункта в шифровальном материале.

Конец сообщения указывается цифрами 70.

Д. Затем передается серия точек (около 5 секунд) и длинное тире.

Е. Затем все сообщение повторяется с немного повышенной скоростью передачи.

4) После повторения сообщения повторяются позывные, затем передается 31, обозначающее конец передачи.

5) Если по каким-либо причинам в течение контакта передача обрывается, то передатчик возобновит передачу серией точек и длинным тире, а потом повторением последней переданной группы до обрыва.

6) Таблица заменителей:

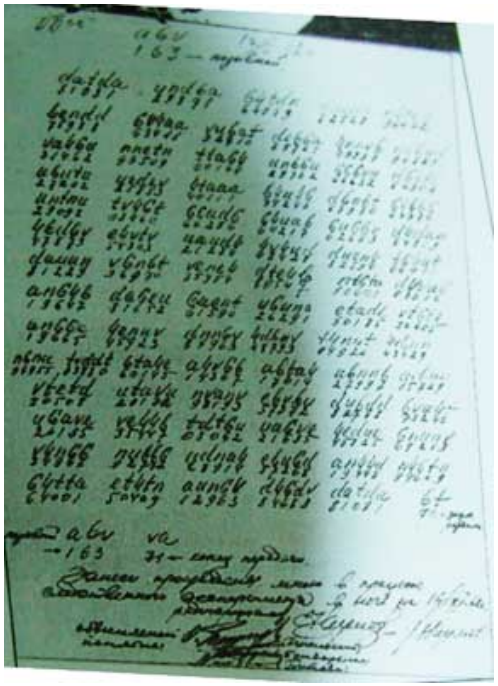
-	0	1	2	3	4	5	6	7	8	9
-	А	Е	И	Н	О	С	Т			
7	Б	В	Г	Д	Ж	З	И	К	Л	М
8	П	Р	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
9	Ы	Ь	Э	Ю	Я	*95*	*96*	*97*	*98*	*99*

95 – точка;
96 – переход на/из латинскую азбуку;
97 – повторяю;
98 – запятая;
99 – начало\конец цифрового текста.

Цифры: 1*1, 2*2, и т.п.

Английские заменители: A – 01, B – 02, C – 03 и т.п.»

В ночь на 16 ноября 1962 года был проведен следственный эксперимент по приему Пеньковским шифротелеграммы от американского разведцентра. В ходе эксперимента был составлен специальный протокол, фотокопия которого приводится ниже:



Здесь мы видим полное соответствие инструкции Пеньковского и её фактического исполнения:

Позывной агента – 163, конец сообщения – 70, конец передачи – 31. Начальная и последняя пятизначные группы криптограммы 81081. Первые две цифры начинаются на 8 – то есть шифрограмма «боевая», а не ложная. 081 – в документе действительно 81 группа цифр + две группы (81081), не являющиеся шифром.

При приеме телеграммы Пеньковский на слух выписывал буквы и цифры, соответствующие латинской азбуке Морзе:

A точка, тире - 1;
U точка, точка, тире – 2;
V точка, точка, точка, тире – 3;
4 точка, точка, точка, точка, тире – 4;
E точка -5;
6 тире, точка, точка, точка, точка – 6;
B тире, точка, точка, точка – 7;
D тире, точка, точка – 8;
N тире, точка - 9;
T тире – 0.

А затем уже переводил их в цифры согласно данной ему инструкции. Таблица же заменителей шифруемых знаков, очевидно, построена по методу советской разведки и в этом не остается никаких сомнений! Сначала в ней выписаны наиболее встречаемые буквы русской азбуки, а затем все остальные. Полностью продублированы знаки пунктуации и условные обозначения. Стоит только сравнить этот ключ с перешифровальной табличкой Вика из 1957 года.

В дальнейшем ЦРУ расширит ассортимент своих таблиц преображения и уже в 70-е годы прошлого века они стали иметь следующий вид (рядом дана табличная реконструкция ключа):

Таблица заменителей (русский алфавит)

-	0	1	2	3	4	5	6	7	8	9
-	**А**	**Е**	И	Н	**О**	С	**Т**			
7	**Б**	В	**Г**	**Д**	Ж	З	Й	**К**	**Л**	**М**
8	**П**	Р	У	Ф	Х	Ц	Ч	Ш	Щ	Ы
9	Ь	Э	Ю	Я	**94**	**95**	**96**	**97**	**98**	**99**

Таблица заменителей (латинский алфавит)

-	0	1	2	3	4	5	6	7	8	9
-	**A**	**E**	N	R	**O**	I	**T**			
7	**B**	C	**G**	**D**	F	H	J	**K**	**L**	**M**
8	**P**	Q	S	U	V	W	X	Y	Z	
9					**94**	**95**	**96**	**97**	**98**	**99**

94 –begin\end figures (начало\конец цифр).

95 – period (пауза в конце предложения, точка).

96 – comma (запятая).

97 – question (вопрос).

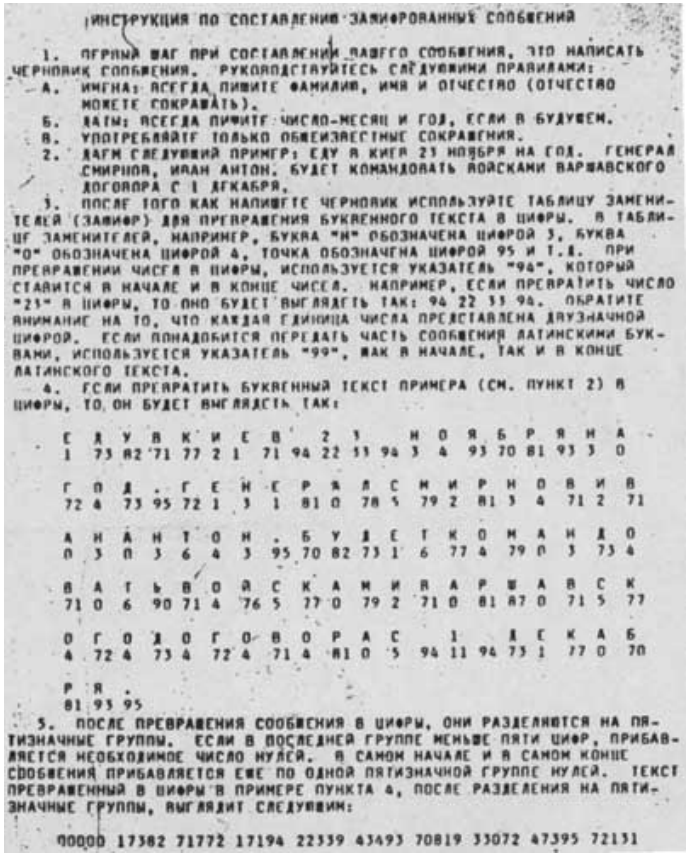
98 – dash (тире).

99 - begin\end (начало\конец русской или латинской азбуки).

Заменители цифр: 1=11; 2=22; 3=33 и т.д.»

Любопытно, что в англоязычной таблице принцип частоты букв соблюдён не полностью. Это связано со стремлением авторов шифра похожие по звучанию русские и латинские буквы обозначать одинаковыми цифрами. Американские разведчики снабжали своих агентов сразу двумя таблицами – для зашифровки и расшифровки криптограмм. В первой табличке супротив букв упорядоченного алфавита выписывались соответствующие им цифрообозначения, а во второй - наоборот. Последнюю табличку мы и приводим в нашей статье. Делалось это для облегчения и без того сложной жизни шпионов.

В нашем распоряжении нет «Правил набора открытого смыслового текста» самого Пеньковского. Но они были типовыми для всех американских агентов. Поэтому и выглядели примерно так:



ИНСТРУКЦИЯ ПО СОСТАВЛЕНИЮ ЗАШИФРОВАННЫХ СООБЩЕНИЙ

1. ПЕРВЫЙ ШАГ ПРИ СОСТАВЛЕНИИ ВАШЕГО СООБЩЕНИЯ, ЭТО НАПИСАТЬ ЧЕРНОВИК СООБЩЕНИЯ. РУКОВОДСТВУЙТЕСЬ СЛЕДУЮЩИМИ ПРАВИЛАМИ:
   А. ИМЕНА: ВСЕГДА ПИШИТЕ ФАМИЛИЮ, ИМЯ И ОТЧЕСТВО (ОТЧЕСТВО МОЖЕТЕ СОКРАЩАТЬ).
   Б. ДАТЫ: ВСЕГДА ПИШИТЕ ЧИСЛО-МЕСЯЦ И ГОД, ЕСЛИ В БУДУЩЕМ.
   В. УПОТРЕБЛЯЙТЕ ТОЛЬКО ОБЩЕИЗВЕСТНЫЕ СОКРАЩЕНИЯ.
2. ДАЛЕЕ СЛЕДУЮЩИЙ ПРИМЕР: ЕДУ В КИЕВ 23 НОЯБРЯ НА ГОД. ГЕНЕРАЛ СМИРНОВ, ИВАН АНТОН, БУДЕТ КОМАНДОВАТЬ ВОЙСКАМИ ВАРШАВСКОГО ДОГОВОРА С 1 ДЕКАБРЯ.
3. ПОСЛЕ ТОГО КАК НАПИШЕТЕ ЧЕРНОВИК ИСПОЛЬЗУЙТЕ ТАБЛИЦУ ЗАМЕНИТЕЛЕЙ (ЗАШИФР) ДЛЯ ПРЕВРАЩЕНИЯ БУКВЕННОГО ТЕКСТА В ЦИФРЫ. В ТАБЛИЦЕ ЗАМЕНИТЕЛЕЙ, НАПРИМЕР, БУКВА "Н" ОБОЗНАЧЕНА ЦИФРОЙ 3, БУКВА "О" ОБОЗНАЧЕНА ЦИФРОЙ 4, ТОЧКА ОБОЗНАЧЕНА ЦИФРОЙ 95 И Т.Д. ПРИ ПРЕВРАЩЕНИИ ЧИСЕЛ В ЦИФРЫ, ИСПОЛЬЗУЕТСЯ УКАЗАТЕЛЬ "94", КОТОРЫЙ СТАВИТСЯ В НАЧАЛЕ И В КОНЦЕ ЧИСЕЛ. НАПРИМЕР, ЕСЛИ ПРЕВРАТИТЬ ЧИСЛО "23" В ЦИФРЫ, ТО ОНО БУДЕТ ВЫГЛЯДЕТЬ ТАК: 94 22 33 94. ОБРАТИТЕ ВНИМАНИЕ НА ТО, ЧТО КАЖДАЯ ЕДИНИЦА ЧИСЛА ПРЕДСТАВЛЕНА ДВУЗНАЧНОЙ ЦИФРОЙ. ЕСЛИ ПОНАДОБИТСЯ ПЕРЕДАТЬ ЧАСТЬ СООБЩЕНИЯ ЛАТИНСКИМИ БУКВАМИ, ИСПОЛЬЗУЕТСЯ УКАЗАТЕЛЬ "99", ЖАК В НАЧАЛЕ, ТАК И В КОНЦЕ ЛАТИНСКОГО ТЕКСТА.
4. ЕСЛИ ПРЕВРАТИТЬ БУКВЕННЫЙ ТЕКСТ ПРИМЕРА (СМ. ПУНКТ 2) В ЦИФРЫ, ТО ОН БУДЕТ ВЫГЛЯДЕТЬ ТАК:

С	Д	У	В	К	И	Е	В	2	3	Н	О	Я	Б	Р	Я	Н	А
1	73	82	71	77	2	1	71	94	22	33	94	3	4	93	70	81	93	3	0

Г	О	Д	.	Г	Е	Н	Е	Р	А	Л	С	М	И	Р	Н	О	В	И	В
72	4	73	95	72	1	3	1	81	0	78	5	79	2	81	3	4	71	2	71

А	Н	А	Н	Т	О	Н	.	Б	У	Д	Е	Т	К	О	М	А	Н	Д	О
0	3	0	3	6	4	3	95	70	82	73	1	6	77	4	79	0	3	73	4

В	А	Т	Ь	В	О	Я	С	К	А	М	И	Я	А	Р	М	А	В	С	К
71	0	6	90	71	4	76	5	77	0	79	2	71	0	81	87	0	71	5	77

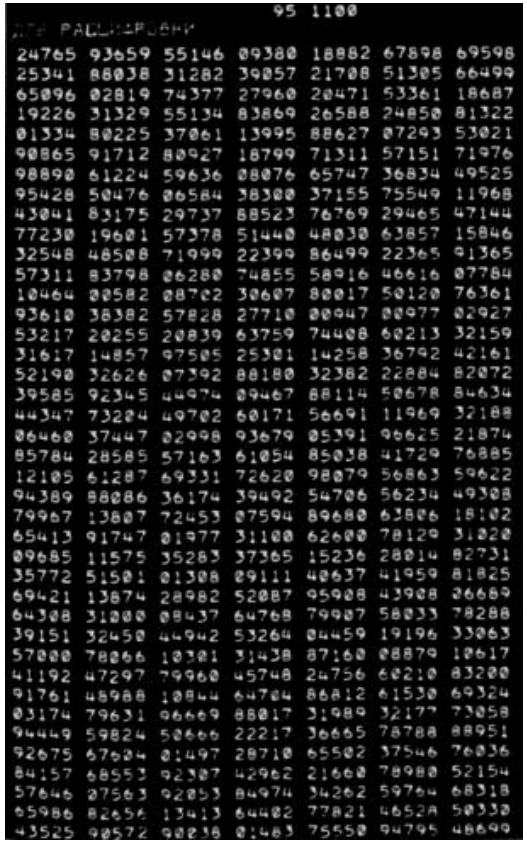
О	Г	О	Д	О	Г	О-	В	О	Р	А	С		1		Д	Е	К	А	Б
4	72	4	73	4	72	4	71	4	81	0	5	94	11	94	73	1	77	0	70

Р	Я	.
81	93	95

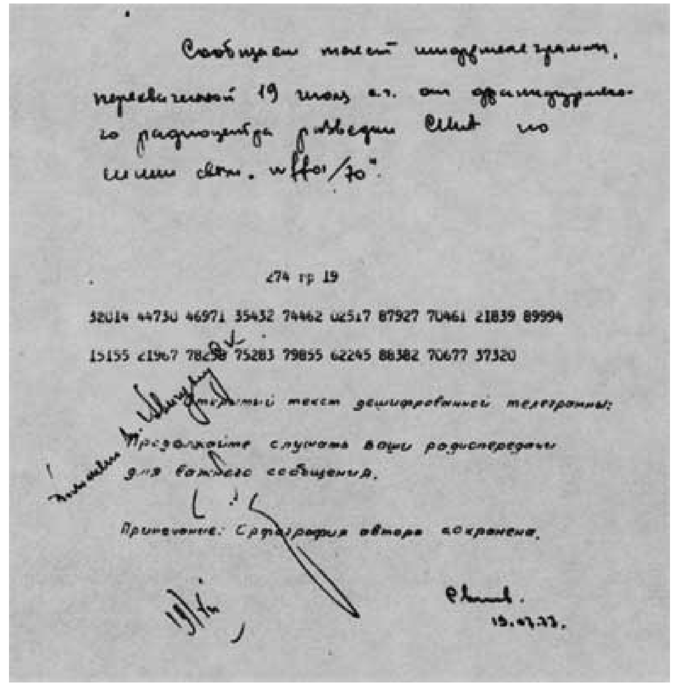
5. ПОСЛЕ ПРЕВРАЩЕНИЯ СООБЩЕНИЯ В ЦИФРЫ, ОНИ РАЗДЕЛЯЮТСЯ НА ПЯТИЗНАЧНЫЕ ГРУППЫ. ЕСЛИ В ПОСЛЕДНЕЙ ГРУППЕ МЕНЬШЕ ПЯТИ ЦИФР, ПРИБАВЛЯЕТСЯ НЕОБХОДИМОЕ ЧИСЛО НУЛЕЙ. В САМОМ НАЧАЛЕ И В САМОМ КОНЦЕ СООБЩЕНИЯ ПРИБАВЛЯЕТСЯ ЕЩЕ ПО ОДНОЙ ПЯТИЗНАЧНОЙ ГРУППЕ НУЛЕЙ. ТЕКСТ ПРЕВРАЩЕННЫЙ В ЦИФРЫ В ПРИМЕРЕ ПУНКТА 4, ПОСЛЕ РАЗДЕЛЕНИЯ НА ПЯТИЗНАЧНЫЕ ГРУППЫ, ВЫГЛЯДИТ СЛЕДУЮЩИМ:

00000 17382 71772 17194 22339 43493 70819 33072 47395 72131

Не правда ли, и это все мы уже знаем. Например, из правил составления шифрованных текстов в операции «Венона». Кстати, добавляемые в шифровке пять нулей в начале и конце текста при сложении с перешифровальными группами из шифровального блокнота дадут истинные цифрогруппы. Таким образом, при разборе текстов было ясно, где начиналась шифровка по странице одноразового блокнота и где она заканчивалась. Сам же этот шифроблокнот американского образца (вернее одна из его страниц) имел следующий вид:



Нам не ведомо, о чем идет речь в шифрограмме, которую американский разведцентр передал Пеньковскому. У нас нет соответствующей страницы его шифроблокнота. Но мы располагаем не менее интригующим документом – копией телеграммы ЦРУ от 19 июля 1977 года к известному их агенту Александру Огороднику (радиопозывной - 274), о котором «ТАСС был уполномочен сообщить». После разоблачения шпиона, не зная его судьбу (как и в случае с Пеньковским!), хозяева продолжали слать ему свои телеграммы:


274 гр 19

32014 44730 46971 35432 74462 02517 87927 70461 21839 89994

15155 21967 78258 75283 79855 62245 88382 70677 37320

Открытый текст дешифрованной телеграммы:

Продолжайте слушать ваши радиопередачи для важного сообщения.

Примечание: Орфография автора сохранена.

Этот документ позволяет провести нам занимательный эксперимент. Заменим текст телеграммы «Продолжайте слушать ваши радиопередачи для важного сообщения» на цифровые обозначения согласно американских инструкций. Получим следующее:

80 81 4 73 4 78 74 0 76 6 1 5 78 82 87 0 6 90 71 0 87 2 81 0 73 2 4 80 1 81 1 73 0 86 2 73 78 93 71 0 74 3 4 72 4 5 4 4 70 88 1 3 2 93 95

Добавив нулевые группы и разбив цифры по пять знаков, получаем искомую криптограмму:

00000 80814 73478 74076 61578 82870 69071 08728 10732 48018 11730 86273 78937 19743 47245 44708 81329 39500 00000

Теперь сюда нужно приплюсовать цифрогруппы из шифроблокнота, но, во первых, у нас его нет, а во вторых, количество цифр в шифровке после этой операции не изменится. Поэтому мы в итоге все равно имеем 19 пятизначных групп, как и указано в шифрограмме. Проведем статистический анализ. Всего в тексте 55 знаков, включая точку. Для их зашифровки потребовалось 83 цифры (исключая добавленные нули). Но если бы тот же самый текст мы шифровали двузначными группами, то на это потребовалось 110 цифр. Таким образом, используя пропорциональный шахматный шифр, мы получили экономию текста в 25%! Кроме того, подобные таблицы значительно усложняют возможный взлом текста, не давая криптологам изначально правильно идентифицировать цифры криптограммы. Повторюсь, что эта красивая идея стала настоящим прорывом в криптографии первой трети XX века, и она принадлежала советским специалистам!

Вот ещё один характерный пример: табличка заменителей букв агента ЦРУ уже в ГДР (немецкий алфавит):

1-A 70-L 80-N 90-/ 00-0
2-N 71-Ä 81-M 91-X 01-1
3-R 72-B 82-O 92-Y 02-2
4-E 73-C 83-Ö 93-Z 03-3

5-I 74-D 84-P 94-, 04-4
6-S 75-F 85-Q 95-. 05-5
76-G 86-T 96-? 06-6
77-H 87-U 97-! 07-7
78-J 88-Ü 98-() 08-8
79-K 89-V 99-- 09-9

При некотором различии, мы опять видим всё те же подходы в организации шифровальной связи американских шпионов. ЦРУ вовсю использовало опыт своих противников в собственной шпионской деятельности по всему миру, беззастенчиво доходя здесь или до прямого плагиата, или синтезируя огромный опыт советских спецслужб.

Обратим своё внимание на следующий характерный факт. Советские разведчики, несмотря на общие подходы в построении таблиц преображения знаков и правил двойной перешифровки, стремились их всячески разнообразить. Но у американских агентов все таблички заменителей были практически одинаковы. И в этом, безусловно, присутствует своя логика. Шпионы ЦРУ были полностью переведены на одноразовые шифрблокноты – наиболее эффективный и простой способ достижения криптостойкой связи. И одновременно – самый затратный и очень опасный. Поэтому по правилам полагалось уничтожать использованные шифространицы сразу после разбора телеграмм. Даже в случае провала агента, ни одна дешифровальная служба противника не сумеет тогда прочесть ранее перехваченные радиограммы. Пойманный шпион ничем здесь уже не мог помочь при всем своем возможном желании – в руках контрразведки не было этих самых нужных страниц. Поэтому и бояться одинаковых таблиц замены букв американцам не приходилось.

Но и на старуху бывает проруха. Эту русскую пословицу подтвердил знакомый нам агент Огородник. При его аресте и обыске квартиры 22 июня 1977 года советские контрразведчики нашли шифровальный блокнот с кодом передач из разведцентра во Франкфурте. К величайшему удивлению следователей, были обнаружены рассованные по различным книгам листы блокнота уже расшифрованных передач. Поразительно, но американский агент не уничтожал их, вопреки строжайшей инструкции. Зачем он это делал, арестованный объяснить не успел, отравившись прямо во время обыска. Самонадеянность Огородника позволила КГБ тут же прочесть часть его шифропереписки, которая была перехвачена за годы поиска этого опасного шпиона.

Кстати, кое-что об этих самых передачах разведцентра. Как мы знаем, агент Пеньковский принимал их еще на слух, используя азбуку Морзе. В 70-е годы прошлого века задачу шпионам значительно упростили. Вот еще одна американская инструкция, датированная 1974 годом и выданная шпиону А.Б.Нилову - инженеру кафедры физики одного из высших учебных заведений Москвы:

«Дважды в неделю во вторник и в четверг в 10 часов вечера на двух частотах из Франфуркта на Майне будут передоваться шифрограммы. Ровно в 22 часа по московскому времени на одной или другой частоте прозвучат позывные, которые повторятся 3 раза. Потом последуют цифры: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0. Все это будет передаваться в течении 10 минут. После этого передадут 10 тональных сигналов, каждый продолжительностью в 1 секунду. Вслед за этим голос произнесет слово: «группен» и назовет количество групп в сообщении. После окончания передачи всех групп будет произнесено слово «видерхолен» и сообщение повторится. Конец передачи будет обозначен словом «энде»».

Таким образом, радиопередачи ЦРУ шли в вечернее время на немецком языке. Диктор первоначально зачитывал цифры трехзначного позывного, по которому определялось - "боевое" это сообщение или "пустышка". После этого диктовались цифры от 0 до 10 для того, чтобы агенту можно было лучше настроиться на прием, а заодно и "потренировать ухо". К тому же под руками у шпионов был уже магнитофон, значительно упрощающий приём радиотелеграмм.

Для подготовки этого очерка я пользовался доступными в прессе материалами о многих американских

агентах прошлого. И все время ловил себя на мысли, что писал как будто про одного единственного шпиона. Настолько они все похожи и одинаковы. И удивительно скучны. Американцы плодили им свои инструкции под копирку, уверяя каждого в отдельности, что думают только о безопасности агента. Но подобная шаблонность вряд ли вела к этой самой безопасности. Об этом говорит печальная судьба каждого из шпионов. У всех их во время арестов находили совершенно одинаковые шифровальные средства – и характерный почерк ЦРУ сразу был на лицо. А если бы эти злополучные агенты ещё знали, что их шифры прямо срисованы американцами с шифров разведчиков их собственной страны, то, наверное, удивились бы и расстроились. Ведь представить этих «любителей» Родины в одном ряду с Зорге, Радо, Треппером, Абелем и с десятками других советских разведчиков совершенно невозможно. Поэтому первые – обычные, презираемые всеми изменники, а героизм вторых удивлял и удивляет весь мир.

Здесь читайте:

"Лица в штатском" (биографический указатель).

СТАТЬИ НА ИСТОРИЧЕСКИЕ ТЕМЫ

Проект ХРОНОС существует с 20 января 2000 года,

на следующих доменах:
www.hrono.ru
www.hrono.info
www.hronos.km.ru,

Редактор Вячеслав Румянцев

При цитировании давайте ссылку на ХРОНОС