«Открытые системы», № 10-2004

Colossus, победивший Lorenz

Леонид Черняк

В первой половине XX века было выпущено невероятное множество типов самых разнообразных механических шифраторов. Их производили в СССР, Японии, США, Великобритании и в ряде других стран.

Некоторые модели были изготовлены в количествах, измеряемых десятками тысяч экземпляров. Рекорд принадлежит американскому шифратору M-209, созданному Борисом Хогелиным, человеком с удивительной биографией, урожденным шведом, проведшим детство в России, работавшим во Франции (кстати, некоторые авторы считают Хогелина белоэмигрантом, но это очевидная ошибка).

Трудно себе представить, но всего было выпущено свыше 140 тыс. экземпляров этого компактного прибора. По воле судеб среди всего этого разнообразия наибольшую известность приобрели немецкие машины, не отличавшиеся какими-то особенными конструктивными или функциональными преимуществами. Своей популярностью эти машины обязаны, скорее, успехам англичан — а в последующем, и американцев — в расшифровке закодированных с их помощью сообщений. Открывшаяся перед союзниками возможность получения засекреченной информации стала немаловажным фактором для поражения фашизма во Второй мировой войне. Одна из немецких шифровальных машин, знаменитая Enigma, стала символом эпохи, именем нарицательным. Центр расшифровки перехваченных английскими спецслужбами радиограмм располагался неподалеку от Лондона, в поместье Бличли-Парк. Помимо англичан, в работе над проектом Ultra, который объединил всех, кто боролся с Enigma, участвовали также польские и американские контрразведчики и криптоаналитики. Об этой уникальной победе академических ученых над военными написано множество книг и статей и даже снят художественный фильм.

В тени поединка Ultra против Enigma осталась еще одна немецкая машина — Lorenz, а также не менее захватывающая эпопея противоборства ей. Соответствующие события развернулись в том же Бличли-Парке, но с другими действующими лицами. Они были лишены внешнего драматизма, присущего первому противостоянию: не было захватов кораблей и подводных лодок, ярких примеров личного мужества моряков, наконец, массовости. Но с технической точки зрения, препятствия, которые пришлось преодолеть при покорении Lorenz, были, пожалуй, посложнее.

Для декодирования сообщений, зашифрованных при помощи Lorenz, группа математиков и инженеров сначала построила механическую машину Heath Robinson, а затем несколько модификаций электронно-механической машины Colossus. Это позволило получать сведения о решениях верховного командования Вермахта.

Иногда о Colossus с заметным оттенком сенсационности говорят как об одном из первых компьютеров. Нельзя сказать, что такое утверждение лишено оснований, но стоит признать, что это сложное и весьма таинственное устройство все же не было компьютером в полном смысле этого слова, хотя в нем и имелись электронные схемы, выполнявшие цифровые функции. Если попытаться описать феномен Colossus языком учения Чарльза Дарвина, то его можно отнести к тем видам, которые не получили дальнейшего развития, но существование которых на начальных этапах любого

эволюционного процесса обязательно. Другое дело, что сами создатели уникального инструмента в своих воспоминаниях, написанных десятилетия спустя, никогда не претендовали на приоритет по части изобретения компьютера.
Задержка в рассказах авторов Colossus об ими содеянном вызвана тем, что в послевоенные годы и их самих, и их творение ожидала странная судьба — практически полное забвение вместо заслуженного признания. В 70-е годы справедливость частично восторжествовала: о конструкции Colossus стало известно практически все, но одна тайна все же осталась. Осталось непонятным, по каким необъяснимым причинам сразу же после окончания мировой войны все сведения о нем были строго-настрого засекречены. Документы — как и почти все экземпляры самой машины — оказались немедленно уничтожены. Известно только, что закрытие проекта Colossus осуществлялось по личному распоряжению Уинстона Черчилля. Но чем было вызвано подобное решение, неизвестно. Эту тайну английский премьер-министр унес с собой.

Lorenz, он же Schlusselzusatz 40/42

Немецкое название машины, Schlusselzusatz, можно перевести как «кодирующая приставка». Действительно, Lorenz использовался в качестве дополнения к телетайпу или коротковолновому радиопередатчику. Как и Enigma, в процессе криптования сообщений эта машина использовала набор вращающихся дисков, генерирующий последовательность псевдослучайных чисел на передающей стороне и точно такой же набор дисков, декодирующий сообщение на принимающей стороне. Одинаковая начальная установка дисков обеспечивала соответствие двух последовательностей чисел на обеих сторонах и, следовательно, корректность декодирования.
На этом, собственно, их конструктивная общность заканчивается. Алгоритмы шифрования и способы представления символов в криптомашинах Lorenz и Enigma были совершенно разными. Enigma была относительно простым и массовым изделием; она использовалась на уровне войсковых соединений, кораблей и подводных лодок. Принцип ее работы заключался в том, что посредством вращающихся дисков (их могло быть три или четыре) и еще некоторых других компонентов выполнялась меньшей или большей длины цепочка замены исходного символа азбуки Морзе «случайным». Очевидно, для расшифровки сообщений, закодированных посредством Enigma, оказалось достаточным иметь определенные сведения о начальных установках. Они-то и добывались героическими усилиями разведчиков и военных. А еще была построена машина Bomba, своего рода антипод Enigma. Она тоже имела набор дисков; сложная процедура совместного вращения сотен дисков в соответствии с заданным алгоритмом реализовывала процесс перебора. Диски вращались до тех пор, пока не достигалась заданная ситуация, определяемая как решение — в таком случае машина останавливалась. (Кстати, показанная в известном фильме реконструкция Bomba — один из немногих исторически достоверных эпизодов в этом произведении.)
В отличие от Enigma, машина Lorenz была изделием штучным, она использовалась верховным командованием германской армии и была намного сложнее. Проблема, стоявшая перед английскими криптоаналитиками, усугублялась тем, что в силу высокой секретности и малой распространенности машины в их распоряжении не было — и не могло быть — никаких агентурных данных, физических захватов и радиоперехватов. Борьба с Lorenz была в чистом виде интеллектуальным поединком. Раскрытие секретов Lorenz можно отнести к самым удивительным достижениям Второй мировой войны, поскольку достоверные сведения об этой машине и ее экземпляр попали в руки английских криптоаналитиков лишь по окончании войны, но это не помешало им на протяжении двух с половиной лет вполне успешно читать самые строгие секреты германского командования. Обнаруженный Lorenz оказался очень похожим на Enigma, однако то, что общее число шифровальных дисков в нем составляло 12 (по два логически последовательно соединенных для генерации шифробита на каждый разряд

пятиразрядного кода плюс еще два кодирования сращения сидящих на одном валу пятерок дисков), удалось определить дедуктивным путем.
Начальная установка заключалась в выборе псевдослучайного расположения зубцов на дисках. Первая группа дисков именовалась K (или Chi), вторая S (или Psi), а на приводе располагались «моторные» диски M1 и M2. К i-му разряду кода по модулю два прибавлялся разряд с диска Ki, а затем Si. Дополнительный элемент «случайности» вносился за счет неравномерности вращения осей дисков. В итоге, скажем, для буквы A выполнялись следующие преобразования (последовательность разрядов зеркальная по отношению к традиционной):
Исходный текст A 1 1 0 0 0
Установка диска K 1 0 0 1 0
После первой операции XOR 0 1 0 1 0
Установка диска S 1 1 0 1 1
После второй операции XOR получилась буква Z 1 0 0 0 1.

От первого перехвата до первой расшифровки

Немцы были абсолютно уверены в неуязвимости Lorenz: машина ни при каких обстоятельствах не могла оказаться в руках противников. Однако сам факт ее существования скрыть было невозможно. О существовании машины англичанам стало известно уже в начале 1940 года. Это случилось, когда среди радиоперехватов, выполненных в Бличли-Парке, один из ведущих английских криптоаналитиков Джон Тильман обнаружил необычные сообщения. Ему стало ясно, что сообщения передавались с использованием пятиразрядной таблицы символов, напоминающей хорошо известный телеграфный код Бодо, и можно было предположить, что сообщения кодировались в стиле кодов Вернама. Тильман немедленно передал свои сведения коллегам в Бличли-Парк, где шифровальной машине было присвоено кодовое имя Fish («Рыба»), а данному типу сообщений — Tunny («Тунец»). Тильман разумно рассудил, что до тех пор пока не будет перехвачено отличающееся сообщение с одной кодовой последовательностью, вероятность расшифровки будет нулевой. Оставалось ждать удачного случая. И, несмотря на строжайшие требования, немецкий оператор все же совершил ожидаемую ошибку. Не будь ее, кто знает, произошло бы или нет все дальнейшее.
Это случилось 30 августа 1941 года при передаче сообщения длиной около 4 тыс. символов из Вены в Афины. Получив в ответ из Афин «Не понял, повторите», венский оператор нарушил все возможные инструкции: он не изменил начальную установку шифратора и передал почти то же самое сообщение с несколько измененными аббревиатурами.
Этого было достаточно для того, чтобы начать расшифровку — «коготок увяз, всей птичке пропасть». В итоге появилась возможность узнать, как формируется псевдослучайная последовательность ключа. К Тильману подключился выпускник Кембриджа, молодой математик Билл Тьюти, вместе им удалось за четыре месяца восстановить логическую схему Lorenz. Далее Макс Ньюман предложил создать электромеханическое устройство для декодирования. Устройство, которое назвали Heath Robinson, спроектировал инженер Чарльз Винн-Вильямс. Машину назвали по имени известного художника-карикатуриста Хита Робинсона (1872-1944), рисовавшего, в том числе, и «сумасшедшие машины».
Идея необычной машины заключалась в суммировании по модулю два содержимого перехваченного кода с подготовленной комбинацией ключей. И то, и другое набивалось на перфоленты, служившие входными данными, далее обе ленты склеивались в петлю и циклически вводились в машину. Изюминкой Heath Robinson был сложный процесс синхронизации ввода лент.

Информационные символы		
код	буквы	«цифры»
00100	space	
00011	A	-
11001	B	?
01110	C	:
01001	D	$
00001	E	3
01101	F	!
11010	G	&
10100	H	STOP, конец сообщения
00110	I	8
01011	J	'
01111	K	(
10010	L	)
11100	M	.
01100	N	,
11000	O	9
10110	P	0
10111	Q	1
01010	R	4
00101	S	BELL, звонок телетайпа
10000	T	5
00111	U	7
11110	V	;
10011	W	2
11101	X	/
10101	Y	6
10001	Z	«
Служебные символы		
01000	CR	возврат каретки (Carriage Return)
00010	LF	следующая строка (Line Feed)
11111	LTRS	перевод на буквенный регистр
11011	FIGS	перевод на регистр цифр

Таблица телеграфных кодов Бодо

Над считанными символами с обеих лент выполнялись арифметические операции. Винн-Вильямс одним из первых в мире предложил использовать для сумматоров электронные схемы на газонаполненных лампах — так называемых тиратронах. В июне 1943 года Heath Robinson был доставлен в «барак № 1» Блечли-Парка, началась практическая работа. Она показала, что избранный замысел и алгоритмические основы совершенно адекватны решаемой задаче, но механическая синхронизация перфолент на скорости ввода 1000 символов в секунду не могла быть надежной по определению. Тем не менее, на этой машине удалось отработать процессы ввода и вывода. Однако, для обеспечения надежности нужна была другая машина с меньшим числом механических компонентов. Ею стал Colossus, разработанный совместно Максом Ньюманом и Томми Флоуерсом.

Недолгая, но яркая жизнь

Проектирование новой машины, которая должна была стать наследником Heath Robinson, началось летом 1943 года, а уже в январе 1944-го Mark 1 Colossus, построенный на 1500 лампах, был запущен в эксплуатацию. Он был действительно огромен: состоял из пяти стоек общей длиной 5,5 метров и более 2 метров высотой. В стойках были смонтированы тиратронные цепи, эмулировавшие вращение дисков Lorenz. Архитектура Colossus позволяла обрабатывать перфоленту с шифрованным сообщением со скоростью 5 тыс. символов в секунду; иными словами, на один цикл обработки среднего сообщения уходило не более секунды. Самое же удивительное заключалось в том, что Colossus работал и успешно справлялся с зашифровкой.

Работоспособность Colossus оказалась личной победой Флоуерса. Никто не верил, что при таком количестве ламп удастся сохранить надежность устройства.

Colossus с некоторой натяжкой можно назвать программируемой машиной; в данном случае программирование заключалось в наборе при помощи электрических контактов аналогов дисков Lorenz. По итогам испытания Mark I было построено еще несколько

экземпляров Mark II, производительность которых была выше в пять раз, а затем Mark I были модернизированы и доведены до того же уровня.
В конечном итоге всего было выпущено десять легендарных машин в двух модификациях. Использование Colossus позволило свести время расшифровки немецких радиограмм до часов, что позволило снабжать высшее командование союзников стратегически важной информацией. Известно также, что Флоуерс начал проектировать еще более сложную машину Super Robinson, но проект не удалось завершить. Кончилась война и исчезла потребность в такой разработке.
Начиная с 1991 года, группа энтузиастов взялась за реставрацию Colossus. В мае 2004 года копия Colossus Mk II была установлена в музее Бличли-Парка.

Таблица кодов Бодо и шифрование по Вернаму

В современных системах для представления алфавитно-цифровых данных чаще всего используется кодировка ASCII, где одному символу ставится в соответствие восемь двоичных разрядов. В телеграфных аппаратах использовалась пятидорожечная перфолента, которая ограничивала представление всего 32 символами. Идея создания кодовой таблицы принадлежит французскому инженеру Эмилю Бодо, он выдвинул ее в 1875 году как средство усовершенствования азбуки Морзе, позволившее построить печатающий символы телеграфный аппарат. Первый вариант кодировки в последующем был значительно улучшен и дополнен. В частности, к нему добавился символ, аналогичный современному Caps Lock, который позволил вдвое увеличить количество кодируемых символов. Впрочем, название кодировки осталось прежним.

Коды Бодо

Коды Бодо стали основой для широко распространенной системы шифрования, предложенной двумя американцами, Гилбертом Вернамом и Паркером Хиттом. Система оказалась на редкость проста и надежна. В ее основе лежало удивительное свойство функции XOR (исключающее ИЛИ) — сложение по модулю два. Это свойство заключается в том, что, если дважды к одному и тому же двоичному числу прибавить по модулю два другое двоичное число, то результат будет равен исходному значению. Преобразование открытого текста в коде Бодо в шифрованный текст осуществлялось посредством прибавления по модулю два к каждому исходному разряду одного случайного разряда ключа шифрования. Скажем, буква Y в коде Бодо имеет код 10101, к ней прибавляется кодовый ключ 10010 и получается шифросимвол 00111. Чем случайнее кодовые ключи, тем выше устойчивость такого метода кодирования к несанкционированному распознаванию. Это было продемонстрировано автором теории передачи данных Клодом Шенноном в 1949 году. Однако сложность кодирования по Вернаму заключается в том, что использование шифра Вернама приводит к значительной временной избыточности, так как длина кода открытого текста равна длине кода зашифрованного текста и, кроме того, такое кодирование требует высокой степени контроля хранения, транспортировки и уничтожения ключей. С последней сложностью чаще всего сталкивались агенты КГБ, где было принято использование специальных шифроблокнотов с заранее подготовленными последовательностями случайных чисел; они печатались на особой бумаге с добавлением целлулоида, которая сгорала мгновенно и практически без пепла. Сложности, связанные с использованием шифроблокнотов, искупались надежностью — но до тех пор, как они не попадали в руки контрразведки, как это случилось при аресте Рудольфа Абеля.