Хронология расшифровки

Эта хронология расшифровки попытки, задача декодирования как понятно последовательность отдельных процессов для идентификации.

В основе этого представления на события используются для расшифровки "Энигма (Enigma)." Этот эксперимент ряд публикаций в качестве основы. В то же время, эта группа вопросов, которые в современной литературе остается открытым для расшифровки есть.

По этой хронологии , отдельные этапы процесса в хронологическом порядке рассматриваются.

Это только разбить его на отдельные процессы, отношения четко показано на рисунке.

Процесс шифрования Передатчик - приемник	Процесс декодирования третьей стороной (деятельности)	Комментарии
Создание информации для шифрования		
Запутывание и сжатия информации с использованием кодовой книги		
Создание шифртекстов (зашифрованный) и ключевая фраза По механическим вклад в устройство шифрования		
Доставка из ключевых текстов и сообщений ключ на радио		
Передачи зашифрованного сообщения радио об «открытом канале радио"		Радио было перехвачено сообщение для всех Место нахождения передатчика может быть

		определена по пеленгации Старая поговорка "искры в государственной измене", и это утверждение верно лишь отчасти.

Процесс шифрования	Процесс декодирования третьей стороной (деятельности)	Комментарии
Отправка зашифрованного сообщения получателю Прием радио шифрованное сообщение получателю	Запись зашифрованное сообщение от прослушивания станций и регистрацию из пяти групп	Начало мероприятия в рамках третьего Требуемое время: Зависит от длины предложения Точность: недостатки; Помех, а также записи ошибки
Перенос зашифрованных сообщений радио расшифровщик	Создание машиночитаемых "зашифрованные телекс радио "в группах по пять	Время передачи: в зависимости от длины говоря, от наличия канала связи (канал телетайпу / телексу.
Расшифровка зашифрованных сообщений беспроводного использования действующими ключами Установка каждой клавиши колес (порядка ключ колеса) Установка колес с помощью ключа ключевое сообщение Установка выделения знака (коммутационной панели)	Передача и прием в "зашифрованные телекс радио Dechiffrierzentrale	Вклад в Dechiffrierzentrale, ожидая открытого Dechiffrierkapaziät

Объем каждого шага было по-другому		
Начало расшифровки зашифрованных сообщений радио	Помощь в расшифровке; сообщение ключ	Дополнительные ресурсы: Координаты станции радиопеленгации Называть Радио оператора , мониторинга специалисты смогли идентифицировать отправителя на основе предоставления азбуки Морзе. Небрежность в выборе ключевых сообщений Стандартная формулировка в виде простого текста. Отверстия , один за другим два одинаковых букв Захваченные ключевые документы и код книги, а также функциональных устройств шифрования (Основные средства разрешено временное мгновенно читать по зашифрованной передачи радио) И другой информации криптографическими
Продолжительность расшифровки: Через несколько минут или меньше	Начало расшифровки	Начало декодирования со стороны третьих лиц задерживается на дополнительные шаги. Преобразование зашифрованного трафика радио в машиночитаемой форме (телекс) Передача в 5 - канал формата (ITA 2)

		Задержка передачи данных на большие объемы сообщений. Причина: Награда будет зашифрован одновременно записаны несколько станций мониторинга, а затем отправлены в Dechiffrierzentrale. Через изображения одного и того же зашифрованное сообщение радио через несколько независимых станций мониторинга, уровень ошибок в процессе декодирования может быть значительно сокращена.
Передача расшифрованные данные на приемник и образцовой информации	Продолжительность расшифровки: За несколько минут до нескольких месяцев или дольше	Продолжительность расшифровки решение о ценности информации
		Для отправителя информации с этого момента информация утратила свое значение
	Успешное дешифрование Подробнее ...	
	Шифрование расшифрованные фразы, с очень безопасная процедура, и только к определенной группе лиц	Обеспечение конфиденциальности, которая решается методом В случае с "Enigma" дальнейших разбирательств в "Ультра"
	Получение информации и	

	инициировать соответствующий ответ, если необходимо	

Эти этапы процесса были необходимы для преодоления системы шифрования на основе электро-механических операций.

1) Прочитайте здесь, чтобы прекрасные представления Нидерланды Музей Crypto. Вы найдете очень хорошо представленной информации. Даже по вопросам шифрования средствами. Существует документированный истории Enigma в Германии, а также различные типы устройств типа. Существует также "вынужденного безделья" британской криптологов показано оборудование изменение подлодки силу. Термин «бездействие» был выбран сознательно, потому что персонал, который работает этих устройств был осужден на бездействие. В отличие от криптологов курили головы. Это привело к более «провала» Dechiffrierzentrale.
2) Это стало возможным в некоторых случаях немедленной расшифровки информации, есть несколько причин: захват немецких подводных лодок и других судов. Или другие, давно поставщик ключевых документов, с тем KL - 7 и другие системы.

Автор: Старый Gocs, Берлин, июнь / июль 2012
Этот материал обновляется знание новых фактов.
Добавлено в www.gocs.de или www.gocs.info