Zeittafel der Entschlüsselung

Dieser Zeittafel der Entschlüsselung stellt einen Versuch dar, die Problematik der Entschlüsselung als eine verständliche Abfolge der Einzelprozesse aufzuzeigen.

Als Grundlage für diese Darstellung sollen die Ereignisse der Entschlüsselung der „Enigma (Rätsel)“ dienen. Diesem Versuch liegen eine ganze Reihe von Veröffentlichungen zu Grunde. Gleichzeitig stellt diese Zeittafel Fragen, die auch in der neueren Literatur zur Entschlüsselung offen geblieben sind.

Für diese Zeittafel werden die einzelnen Prozessschritte in chronologischer Reihenfolge betrachtet.

Denn nur durch die Zerlegung in Einzelprozesse können die Zusammenhänge klar aufgezeigt werden.

Prozess der Verschlüsselung Sender - Empfänger	**Prozess der Entschlüsselung durch den Dritten (Aktivitäten)**	**Bemerkungen**
Erstellung der Information zur Verschlüsselung		
Verschleierung und Komprimierung der Information durch die Verwendung des Codebuches		
Erstellen des Schlüsseltexte (Geheimtextes) und des Spruchschlüssels Durch mechanische Eingabe in das Verschlüsselungsgerät		
Übergabe des Schlüsseltextes und dem Spruchschlüssel an den Funker		
Übermittlung des verschlüsselten Funkspruch über einen „offenen Funkkanal“		Funkspruch wurde für jedermann abhörbar Standort des Senders konnte durch Funkpeilung ermittelt werden

		Alter Ausspruch „Funken ist Landesverrat“; diese Aussage gilt nur bedingt.

Mit den nachfolgenden Prozessschritten kann der „Dritte“ erst aktiv in das Geschehen eingreifen.

Prozess der Verschlüsselung	Prozess der Entschlüsselung durch den Dritten (Aktivitäten)	Bemerkungen
Sendung des verschlüsselten Funkspruch an den Empfänger Empfang des verschlüsselten Funkspruchs durch den Empfänger	**Aufnahme des verschlüsselten Funkspruch durch die Abhörstationen und Protokollierung der Fünfergruppen**	**Beginn der Aktivitäten des Dritten** Erforderliche Zeit: abhängig von der Spruchlänge Fehlerfreiheit : fehlerbehaftet; Funkstörungen; Aufnahmefehler
Übergabe des verschlüsselten Funkspruchs an den Entschlüsseler	Erstellung eines maschinenlesbaren „verschlüsselten Funkfernschreiben“ in Fünfergruppen	Übermittlungsdauer: Abhängig von der Spruchlänge; Von der Verfügbarkeit eines Kommunikationskanals (Fernschreibkanal/ Telex.
Entschlüsselung des verschlüsselten Funkspruchs mittels aktuell gültigem Schlüssel , Einstellung der einzelnen Schlüsselräder(Reihenfolge der Schlüsselräder) Einstellung der Schlüsselräder mittels des Spruchschlüssel Einstellung der Zuordnung der Zeichen (Steckerbrett) Der Umfang der einzelnen Schritte war unterschiedlich	Übermittlung und Empfang des „verschlüsselten Funkspruch“ in der Dechiffrierzentrale	Eingang in der Dechiffrierzentrale; Warten auf freie Dechiffrierkapazität
Beginn der Entschlüsselung des verschlüsselten Funkspruchs	Hilfsmittel bei der Dechiffrierung; **Spruchschlüssel**	**Weitere Hilfsmittel:** Koordinaten des Senders durch **Funkpeilung** **Rufzeichen** **Funker**; Abhörspezialisten konnten die Sender anhand des Gebens der Morsezeichen erkennen. **Nachlässigkeiten** bei der Wahl der Spruchschlüssel Standardformulierungen im Klartext.

		Löcher ; durch zwei gleichlautende Buchstaben hintereinander **Erbeutete Schlüsselunterlagen** und Codebücher sowie funktionsfähige Verschlüsselungsgeräte (Schlüsselmittel erlaubten einen zeitweiliges sofortige mitlesen des verschlüsselten Funkverkehrs) Sowie weitere kryptologische Informationen
Dauer der Entschlüsselung : **Wenige Minuten oder kürzer**	**Beginn der Entschlüsselung**	**Beginn der Dechiffrierung auf der Seite des Dritten verzögert sich durch zusätzliche Schritte.** **Umwandlung des verschlüsselten Funkverkehrs in eine maschinenlesbare Form (Telex)** **Übermittlung im 5 – Kanalformat (ITA 2)** **Verzögerung der Nachrichtenübermittlung bei starken Nachrichtenaufkommen.** **Ursache:** **Der verschlüsselte Spruch wird gleichzeitig von mehreren Abhörstationen aufgenommen und dann an die Dechiffrierzentrale gesendet.** **Durch die Aufnahmen der gleichen verschlüsselten Funksprüche , durch mehrere unabhängiger Abhörstationen, kann die Fehlerrate im Prozess der Entschlüsselung stark reduziert werden.**
Übergabe der entschlüsselten Information an den Empfänger und Ausführung der übermittelten Informationen	**Dauer der Entschlüsselung:** **Wenige Minuten bis zu mehreren Monaten oder auch länger** [1) 2)] **Zur Frage der Dauer der Entschlüsselung liegen keine Informationen vor.** **Wie viel verschlüsselter Sprüche konnten gleichzeitig entschlüsselt werden ?**	**Die Dauer der Dechiffrierung entscheidet über den Wert der Information**

		Für den Sender der „Information“ hat ab diesem Zeitpunkt die Information ihren Wert verloren
	Entschlüsselung erfolgreich Weiter...	
	Chiffrierung des dechiffrierten Spruchs mit einem sehr sicheren Verfahren und nur an einen ausgewählten Personenkreis	**Sicherung des Geheimnisses, das das Verfahren gelöst ist Im Falle „Enigma“ weiter im Verfahren „Ultra“**
	Empfang der Information und Einleitung gegebenenfalls entsprechender Reaktion	Für den „Dritten“ kann erst zu diesem Zeitpunkt eingeschätzt werden. Ob die Information einen Wert hat.

Diese Prozessschritte waren erforderlich, um ein Verschlüsselungssystem auf der Grundlage elektro-mechanischer Funktionsweise zu lösen.

1) Lesen Sie hier zu , die hervorragende Darstellung des Crypto Museum Niederlande. Sie finden dort eine sehr gut dargestellte Information. Auch zu den Fragen der Verschlüsselungsmittel. Dokumentiert ist dort die Geschichte der Enigma in Deutschland sowie die Varianten der verschiedensten Gerätetypen. Dort wird auch die „erzwungene Untätigkeit“ der britischen Kryptologen nach einem Gerätewechsel in der U-Bootwaffe gezeigt. Der Begriff „Untätigkeit“ wurde bewusst gewählt, denn das Personal, das diese Geräte bediente war zur Untätigkeit verurteilt. Dagegen rauchten den Kryptologen die Köpfe. Dies führte zu einem längeren „Ausfall“ der Dechiffrierzentrale.

2) Das in einigen Fällen eine sofortige Entschlüsselung der Informationen möglich war, hat verschiedene Ursachen: Erbeutung deutscher U-Boote oder anderer Schiffe. Oder durch einen langjährigen Lieferanten der Schlüsselunterlagen, so u.a. KL – 7 und weiterer Systeme.

Autor : Old Gocs, Berlin, im Juni/Juli 2012

Dieses Material wird bei Kenntnis neuer Fakten aktualisiert.

Veröffentlicht unter www.gocs.de oder www.gocs.info