

## Panneau de temps du décodage

Ce panneau de temps celui-ci décodage représente une tentative de montrer la problématique du décodage comme une suite compréhensible des processus individuels.

Les événements doivent servir le décodage de l' "Enigma (mystère)" de fondement de cette représentation. Une série entière de publications est à la base de cet essai. Ce panneau de temps pose en même temps des questions qui sont restées ouvertes aussi dans la littérature récente au décodage.

Pour ce panneau de temps, les différents pas de processus sont regardés par une suite chronologique.

Car les rapports ne peuvent être montrés clairement qu'à travers la décomposition dans des processus individuels.

Processus du cryptage Emetteur - destinataire	Processus du décodage par le tiers (activités. )	Des remarques
<b>Construction de l'information sur le cryptage</b>		
Verschleierung et compression de l'information à travers l'utilisation du livre de code		
Faire le textes de clés (texte secret) et de la clé de dicton A travers la requête mécanique dans l'appareil de cryptage		
Remise du texte de clés et la clé de dicton à l'opérateur radio		
Transmission l'ont codé message radio sur un "canal de radio ouvert"		Le message radio devenait abhörbar pour tout le monde L'emplacement de l'émetteur pouvait être déterminé par le relèvement de radio Vieillis de-dicton "est à étincelles trahison" ; cette déclaration n'est valable que conditionnellement.

**Avec les pas de processus suivants, le "tiers" peut intervenir dans les événements d'abord activement.**

Processus du cryptage	Processus du décodage par le tiers (activités.)	Des remarques
Envoi l'ont codé message radio au destinataire Réception du message radio codé par le destinataire	<b>Enregistrement l'ont codé message radio à travers l'Abhörstationen et le Protokollierung des groupes de pièce de cinq pfennigs</b>	<b>Début des activités du tiers</b> Temps nécessaire : Dépendant de la longueur de dicton Liberté de fautes : Faute complet ; Des dérangements de radio ; Faute d'enregistrement
Remise du message radio codé à le décodé	"Des télex de radio codaient de la construction d'un machine lisible" dans des groupes de pièce de cinq pfennigs	Durée de transmission : Dépendant de la longueur de dicton ; De la disponibilité d'un canal de communication (canal de télex/télex.
Décodage du message radio codé au moyen d'une clé qui est actuellement valable, Réglage des différentes roues de clé (suite des roues de clé.) Réglage des roues de clé au moyen de le clé de dicton Réglage du classement des signes (planche de prise.) L'étendue des différents pas était différente	Transmission et réception l'ont "codé message radio dans le bureau central de déchiffrer"	Entrée dans le bureau central de déchiffrer ; Des points de vue sur la capacité de déchiffrer libre
<b>Début du décodage du message radio codé</b>	Instrument de travail au Dechiffrierung ; <b>Clé de dicton</b>	<b>D'autres instruments de travail :</b> Des coordonnées de l'émetteur à travers le <b>relèvement de radio</b> <b>Signe de réputation</b> Opérateur radio ; Les Abhörspezialisten pouvaient reconnaître les émetteurs avec donner les <b>signes</b> d'envoyer un message en morse. Des <b>négligences</b> lors du choix des clés de dicton Des formulations standard dans le texte clair. <b>Des trous ; à travers deux lettres derrière l'un l'autre qui sont même</b> <b>Documents de clé</b> et livres de code <b>emparés</b> ainsi

		<p>qu'appareils de cryptage en état de marche  ( Des moyens de clé en ont permis un avec-lecture immédiate temporaire de la circulation de radio codée.)  Ainsi qu'informations autres kryptologische</p>
<p><b>Durée du décodage :</b>   <b>Plus court peu de minutes n'est-ce pas</b></p>	<p><b>Début du décodage</b></p>	<p><b>Le début du Dechiffrierung sur le côté du tiers est retardé à travers des pas supplémentaires.</b>  <b>Transformation de la circulation de radio codée dans une forme machine lisible (télex. )</b>  <b>Transmission dans cela 5 - format de canal (ITA 2. )</b>  <b>Retard dans des apparitions de nouvelle fortes de la communication.</b></p> <p><b>Cause :</b>  <b>Le dicton codé est accueilli par plusieurs Abhörstationen et il est envoyé ensuite au bureau central de déchiffrer par eux en même temps.</b></p> <p><b>A travers les commencements des mêmes messages radio codés à travers plusieurs d'Abhörstationen indépendants, le Fehlerrate peut être réduit fortement dans le processus du décodage.</b></p>
<p><b>La remise de l'information au destinataire et de l'exécution des informations transmises décodée</b></p>	<p><b>Durée du décodage :</b>  <b>Peu de minutes jusqu'à plusieurs mois de plus</b>  1) 2 )</p> <p><b>Aucune information sur la question n'a été présentée à la durée du décodage.</b>  <b>Comme des dictons beaucoup codés, pouvait-on décoder en même temps?</b></p>	<p><b>La durée du Dechiffrierung décide de la valeur de l'information</b></p>

		<b>Pour l'émetteur de l' "information", l'information a perdu sa valeur à partir de ce moment</b>
	<b>Décodage couronné de succès ***Weiter... ***</b>	
	<b>Procédé et catégorie de personnes seulement choisie à un très sûrs de Dechiffrierung du dicton déchiffré avec l'un</b>	<b>Protection du secret, cela le procédé est résolu Procéder dans cela plus loin dans le cas "Enigma" "Ultra"</b>
	Réception de réaction qui correspond à l'information et à l'introduction le cas échéant	Pour le "tiers", on peut évaluer à ce moment-là d'abord. Si l'information a une valeur.

**Ces pas de processus ont été nécessaires pour résoudre un système de cryptage sur la base de manière de fonction électrique mécanique.**

1. Vous lisez ici à, l'excellente représentation du Crypto de [musée Pays-Bas](#). Vous trouvez une information très bien représentée là-bas. Aussi aux questions des moyens de cryptage. Documente là-bas l'histoire de l'Enigma en Allemagne ainsi que les variantes des types d'appareil les plus différents. Là-bas, l' "inaction forcée" est aussi montrée au Kryptologen britannique après un changement d'appareil dans l'U - Bootwaffe. Le terme "de l'inaction" a consciemment été choisi, car le personnel, qui a utilisé ces appareils a condamné à l'inaction. Ont fumé le Kryptologen contre cela les têtes. Ceci menait à une plus longue "défaillance du bureau central de déchiffrer".
2. Cela un décodage immédiat des informations a été possible, il a différentes causes dans quelques cas : L'Erbeutung des sous-marins allemands ou de d'autres bateaux. Ou par un fournisseur de longue date des documents de clé, si entre autres KL, 7 et autres systèmes.

Auteur : Old Gocs, Berlin en juin 2012./juillet ils

Cette matière est actualisée à la connaissance de nouveaux faits.

Publiez sous [www.gocs.de](http://www.gocs.de) ou [www.gocs.info](http://www.gocs.info)