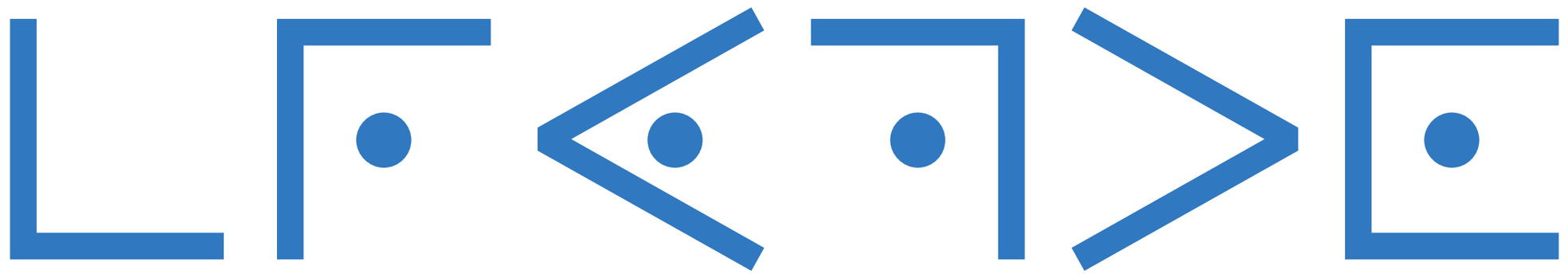


secret parfait

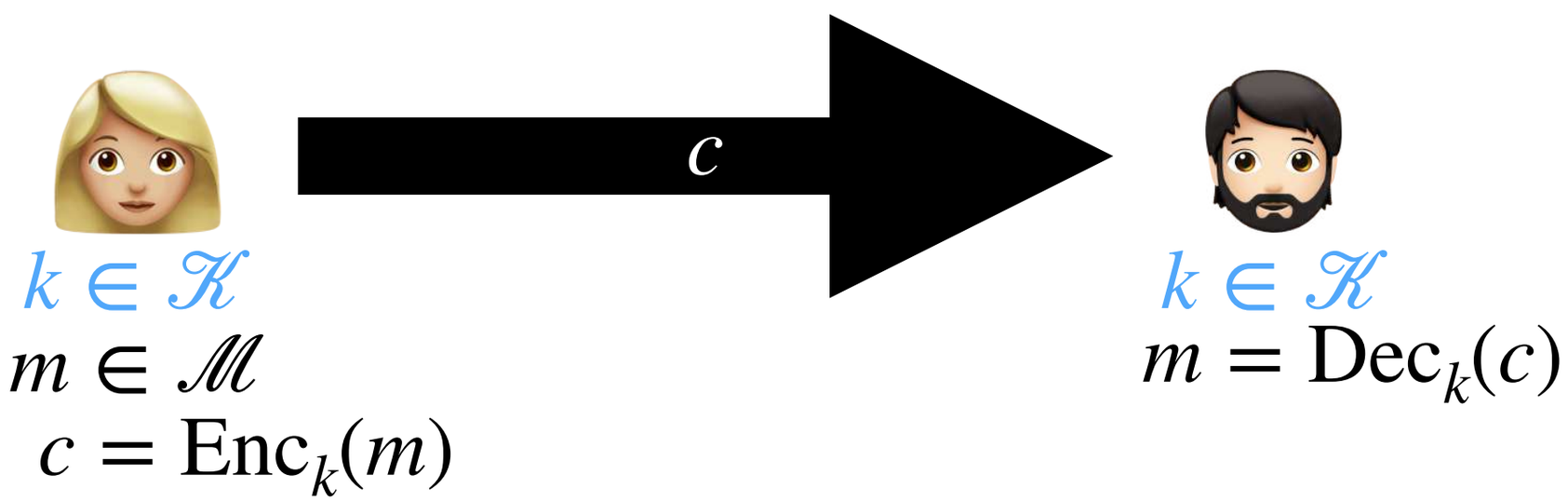
Nicolas Ollinger

M1 informatique — 2024/2025

Cryptographie classique

Historiquement la cryptographie repose sur un secret partagé, une **clé**, échangé à l'avance par les participants.

On parle de **cryptographie à clé secrète** ou encore de **cryptographie symétrique**.



Principe de Kerckhoffs

Auguste Kerckhoffs (1835-1903)

La cryptographie militaire,
Journal des sciences militaires,
vol. IX, pp. 5–38, jan. 1883, pp. 161–191, févr. 1883.

Un système cryptographique doit pouvoir tomber entre les mains de l'ennemi : la **sécurité** doit reposer uniquement sur la **clef**, on doit supposer l'algorithme connu.

Cryptographie à clé secrète

Un schéma de chiffrement à clé secrète est défini par un espace des messages et 3 algorithmes :

$\mathscr{M}$ espace des messages

$\mathrm{Gen}() = k$ algo probabiliste de génération de clé

$\mathrm{Enc}_k(m) = c$ algo probabiliste de chiffrement

$\mathrm{Dec}_k(c) = m$ algo déterministe de déchiffrement

$$\forall k = Gen() \quad \forall m \in \mathscr{M} \quad \mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$$

Algorithmes probabilistes ?

Un algorithme probabiliste A est un algorithme qui peut effectuer des **choix aléatoires** (lancers de pièces deux à deux indépendants) pendant son exécution.

Le résultat du calcul de A(x) n'est plus nécessairement unique, il **possède une certaine probabilité**.

Chiffrement par $\oplus$

Exercice Formalisons le chiffrement par xor en tant que schéma de chiffrement à clé privée.

$$E_k(m) = m \oplus k$$

Cette méthode de chiffrement vous semble-t-elle *sécurisée* ?

Cryptographie moderne

Définir formellement à l'aide de modèles mathématiques précis la notion de **sécurité**.

Identifier clairement et de manière non ambiguë **les hypothèses** (P≠NP, ...)

Démontrer formellement la sécurité plutôt que de poursuivre sur la voie artisanale conception/faille/patch.

Secret parfait

Définir formellement la sécurité

Identifier l'objectif de sécurité d'un schéma de chiffrement. Que veut-on empêcher l'adversaire de réaliser ?

Quels sont les capacités de cet adversaire ?

Essayons de définir la sécurité d'un schéma de chiffrement à clé privée (Gen, Enc, Dec) contre une **attaque à un unique texte chiffré seul**.

« L'adversaire ne peut pas deviner la clé » ?

« L'adversaire ne peut pas retrouver le message en clair » ?

« L'adversaire ne peut pas retrouver n'importe quel caractère du message en clair » ?

« Quelle que soit l'information dont dispose l'adversaire sur le texte en clair, le texte chiffré ne doit pas permettre d'obtenir d'avantage d'information concernant le texte en clair. »

Comment formaliser cet énoncé ?

Rappels de probabilités

Probabilités

Ensemble fondamental : ensemble des résultats possibles d'une expérience.

Événement : tout sous-ensemble S de l'ensemble fondamental.

Un événement est réalisé si le résultat de l'expérience appartient à S.

Combinaisons booléennes d'événements.

Distribution de probabilités

Une **distribution de probabilités** sur S associe une probabilité P(X) à tout événement X de S qui satisfait :

$$\forall X \quad P(X) \in [0,1]$$

$$P(S) = 1$$

si $A \cap B = \varnothing$ alors $P(A \cup B) = P(A) + P(B)$

Variable aléatoire

Une **variable aléatoire** est une variable dont les valeurs sont associées à une probabilité.

$$X : S \to E$$

$$P(X = v) = \sum_{X(s)=v} P(s)$$

Exercice V.A. D somme des valeurs de deux dés à 6 faces, calculer P(D=5).

Probabilité conditionnelle

Probabilité qu'un événement ait lieu sachant qu'un autre a eu lieu :

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}$$

$$P(A \cap B) = P(B \cap A) = P(B)P(A \mid B) = P(A)P(B \mid A)$$

Deux V.A. X et Y sont **indépendantes** si

$$P(X = x \mid Y = y) = P(X = x)$$

Secret parfait (suite)

Notations

Considérons un schéma de chiffrement à clé secrète :

$\mathscr{M}$ espace des messages

$\mathscr{K}$ ensemble de toutes les clés

$\mathscr{C}$ ensemble de tous les messages chiffrés

$\mathrm{Gen}() = k$ algo probabiliste de génération de clé

$\mathrm{Enc}_k(m) = c$ algo probabiliste de chiffrement

$\mathrm{Dec}_k(c) = m$ algo déterministe de déchiffrement

$$\forall k = Gen() \quad \forall m \in \mathscr{M} \quad \mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$$

Ajoutons des probabilités

Soit M la variable aléatoire qui représente le texte du message en clair.

$$M \in \mathscr{M}$$

C'est une distribution de probabilités sur les messages...

$$P(M = \text{"the cake is a lie"}) = 0{,}6$$
$$P(M = \text{"there is no cake"}) = 0{,}4$$

Ajoutons des probabilités

Soit K la variable aléatoire représentant la valeur de la clé.

$$K \in \mathcal{K}$$

$$P(K = k) = P(\text{Gen produit la clé } k)$$

Les variables M et K sont indépendantes. Le choix du message à envoyer ne dépend pas du choix de la clé privée.

Ajoutons des probabilités

On associe une variable aléatoire C au texte chiffré à travers l'expérience suivante :

(a) choisir un message m

(b) générer une clé k avec Gen

(c) calculer c = Enc(k,m)

Secret parfait (informel)

« Quelle que soit l'information dont dispose l'adversaire sur le texte en clair, le texte chiffré ne doit pas permettre d'obtenir d'avantage d'information concernant le texte en clair. »

On suppose que l'adversaire connait la distribution de probabilités de M.

L'observation du texte chiffré ne doit pas modifier cette connaissance.

Secret parfait (formel)

Le schéma de chiffrement (Gen, Enc, Dec) **assure le secret parfait** si quelque soit la distribution de probabilité sur l'espace des messages, quelque soit le message m et quelque soit le message chiffré c de probabilité non nulle, on a

$$P(M = m \mid C = c) = P(M = m)$$

Formulation équivalente

Le schéma de chiffrement (Gen, Enc, Dec) **assure le secret parfait** si quelque soit la distribution de probabilité sur l'espace des messages, quelque soient les message m et m' et quelque soit le message chiffré c, on a

$$P(\mathrm{Enc}_K(m) = c) = P(\mathrm{Enc}_K(m') = c)$$

Formulation « expérimentale »

Un adversaire A choisit deux messages m_0 et m_1 quelconques.

L'un de ces deux messages est choisi uniformément et chiffré en c.

A doit alors deviner si le message chiffré c correspond à m_0 ou à m_1.

Un schéma est **parfaitement indistinguable** si A ne peut pas deviner la bonne réponse avec un probabilité supérieure à 1/2.

Équivalence

Un schéma de chiffrement assure le secret parfait si et seulement si il est parfaitement indistinguable.

Exercice Démontrer que le chiffrement par xor n'est pas parfaitement indistinguable. On considérera l'espace des messages de 2 bits et une période de clé uniforme dans {1,2}.

Méthode du masque jetable

UNITED STATES PATENT OFFICE.

GILBERT S. VERNAM, OF BROOKLYN, NEW YORK, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

SECRET SIGNALING SYSTEM.

1,310,719. Specification of Letters Patent. Patented July 22, 1919.

Application filed September 13, 1918. Serial No. 253,962.

To all whom it may concern:

Be it known that I, GILBERT S. VERNAM, residing at Brooklyn, in the county of Kings and State of New York, have invented certain Improvements in Secret Signaling Systems, of which the following is a specification.

This invention relates to signaling systems and especially to telegraph systems. Its object is to insure secrecy in the transmission of messages and, further, to provide a system in which messages may be transmitted and received in plain characters or a well-known code but in which the signaling impulses are so altered before transmission over the line that they are unintelligible to anyone intercepting them.

The invention is here illustrated as applied to a well-known form of printing telegraph systems but, as will be readily understood, it is applicable to other signaling

tact with the ring 7 and the segmental contacts repectively. When the apparatus is at rest this arm is detained by the latch 12 which may be withdrawn by means of magnet 13 under the control of the operator. The receiving side of the distributer has five segments 1′, 2′, 3′, 4′ and 5′, corresponding to the five sending segments but shortened to receive only the central part of the current impulses transmitted. It also has a contact 6′, upon which the distributer arm normally rests, and a contact P for controlling the energization of a relay whose purpose will appear hereinafter. The receiving distributer arm 10′ carries a brush 11′ and is controlled by a latch 12′ and magnet 13′ as in the case of the transmitting distributer arm.

The "sending relays" commonly used in the form of printing telegraph system here shown are indicated at 14, 15, 16, 17 and 18,

Schéma du masque jetable

Pour une valeur de n fixée. L'espace des messages, des clés et des textes chiffrés est $\{0,1\}^n$.

Gen choisit **uniformément** une clé.

Enc calcule le **xor** du message et de la clé.

Dec calcule le **xor** du message et de la clé.

Théorème(Shannon 1949) Le masque jetable assure le secret parfait.

Attention !

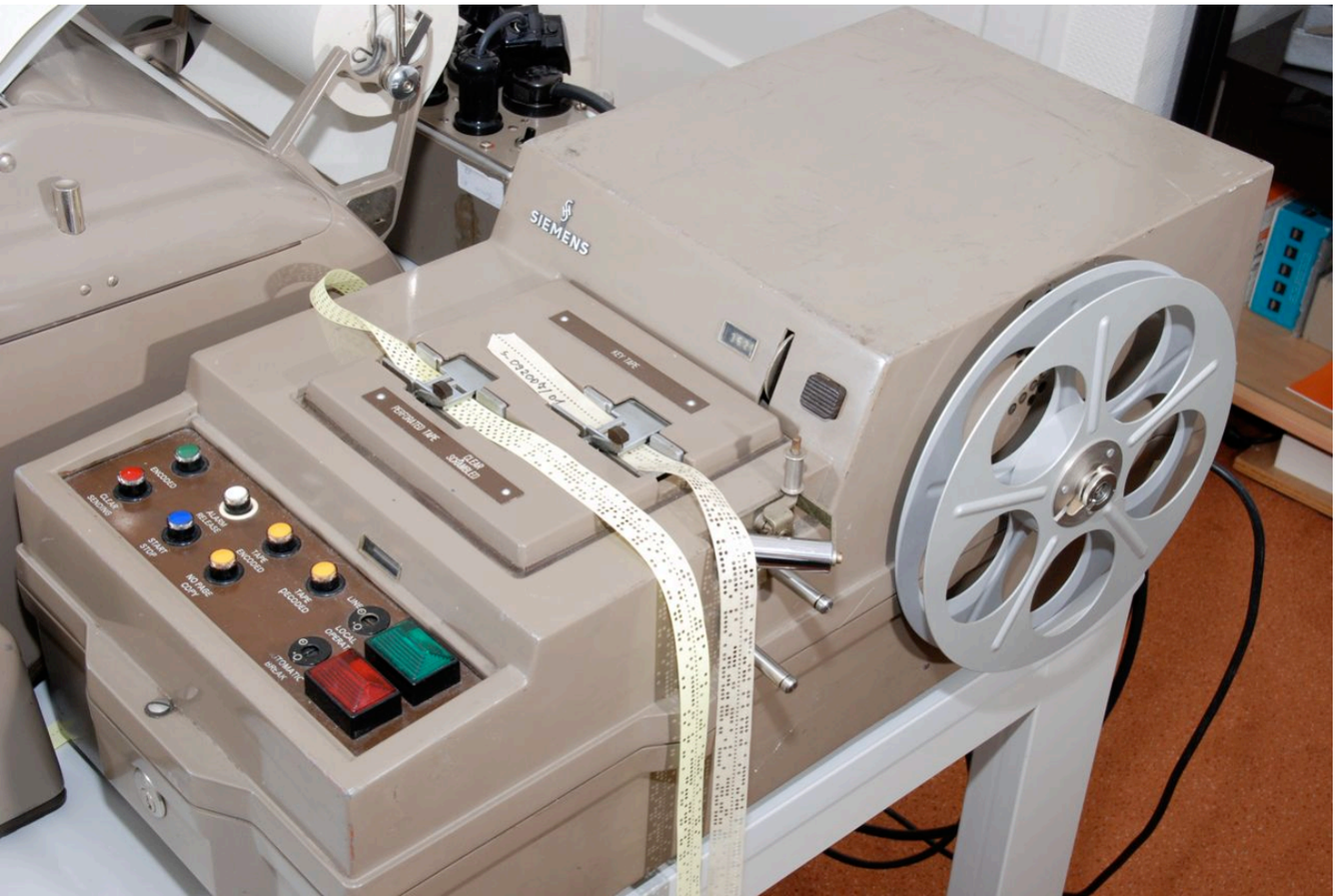
Pour que l'utilisation du masque jetable assure le **secret parfait** en pratique il faut :

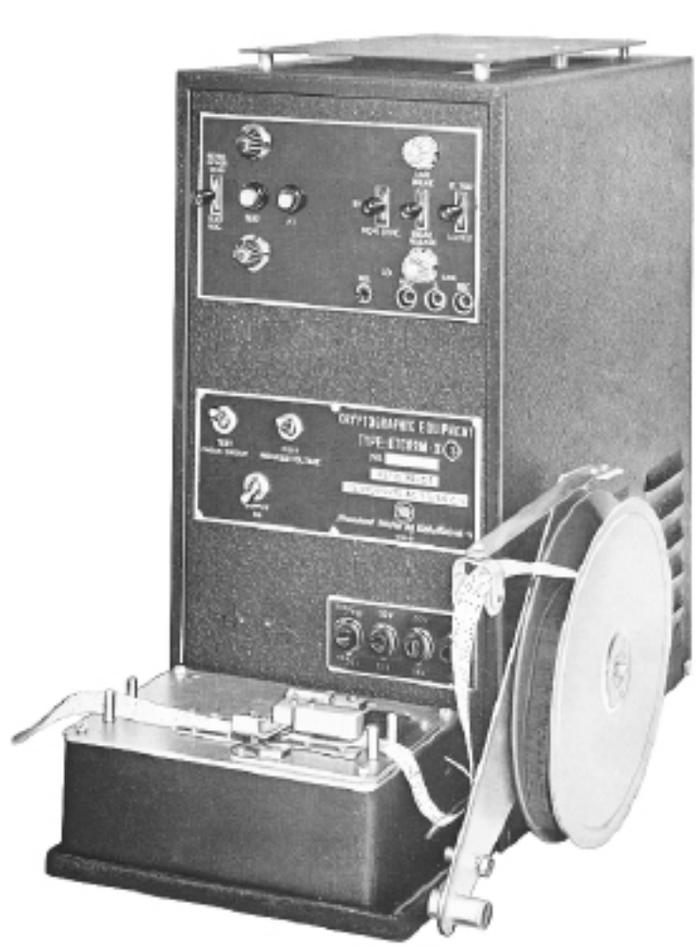
1. que la clé soit réellement aléatoire ;
2. utiliser la clé une seule fois ;
3. transmettre la clé par un canal sécurisé ;
4. détruire la clé après utilisation.

Le téléphone rouge ☎

Teletype installé entre Moscou et Washington en juillet 1963 après la crise des missiles de Cuba.

Échange de masques jetables par valises diplomatiques.





Communication Theory of Secrecy Systems*

By C. E. SHANNON

1 INTRODUCTION AND SUMMARY

The problems of cryptography and secrecy systems furnish an interesting application of communication theory[1]. In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography[2]. There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech in-

Limitations du secret parfait

Théorème Si (Gen, Enc, Dec) assure le secret parfait alors l'espace des clés est au moins aussi grand que l'espace des messages.

Théorème(Shannon) Si la taille des trois espaces (messages, clés, chiffrés) est égale le schéma assure le secret parfait si et seulement si :

1. toutes les clés sont équiprobables ;
2. pour tout message m et tout chiffré c il existe une unique clé k telle que Enc(k,m)=c.

Secret imparfait

Sécurité calculatoire

Remplacer le secret parfait par un secret relatif à la puissance de calcul bornée de l’attaquant.

Une méthode de chiffrement est sûre si le meilleur algorithme pour casser le chiffre nécessite un nombre d’opérations trop grand pour être utilisable en pratique.

Principes de Shannon

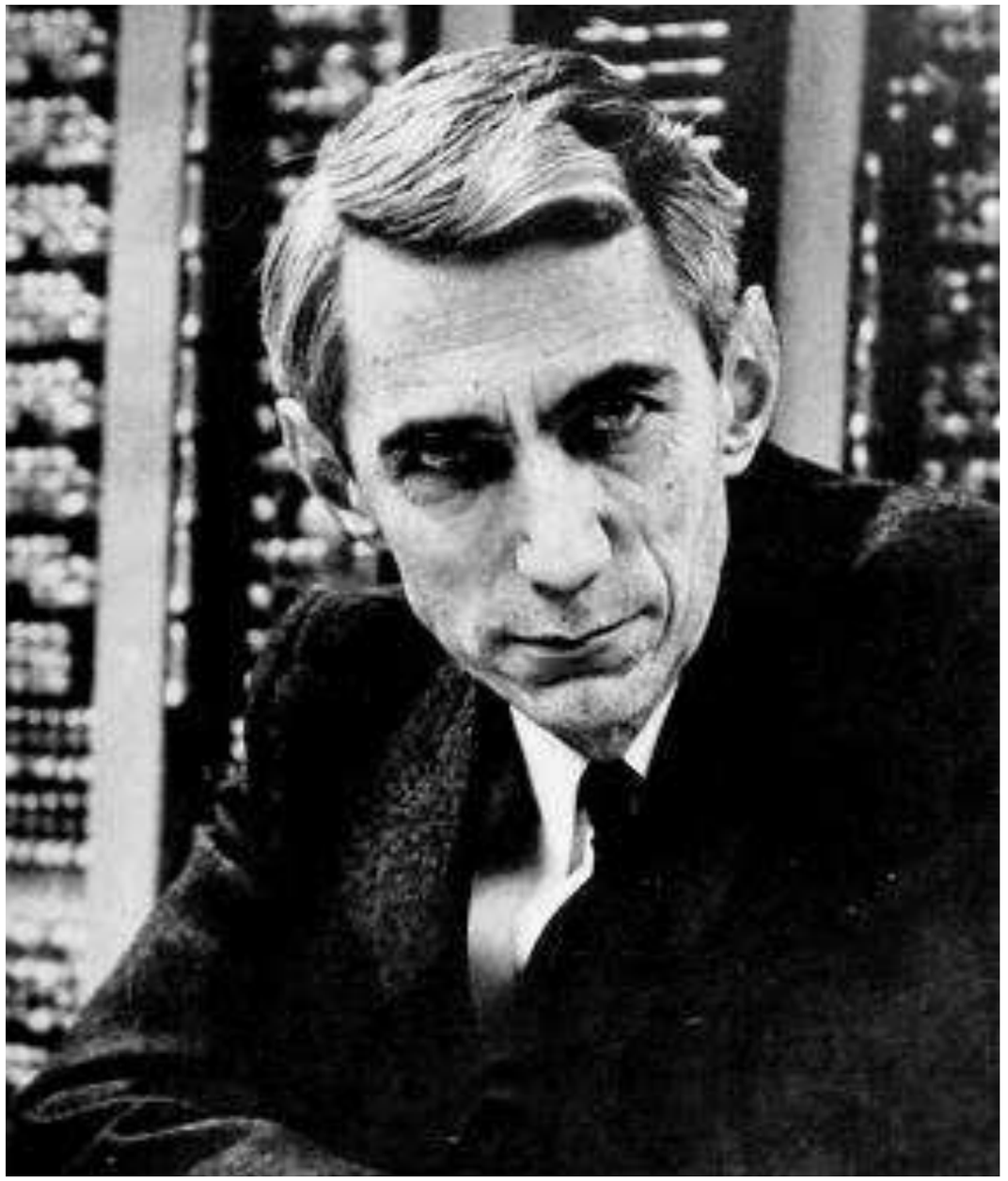
Claude Shannon (1916-2001)

Communication Theory of Secrecy Systems, Bell System Technical Journal, vol. 28(4), page 656–715, 1949.

Diffusion : mélanger l'information du message en clair dans le message chiffré.

Confusion : utiliser la clef pour camoufler le message en clair.

Effet d'avalanche : modifier un bit en entrée peut modifier tous les bits de la sortie.



Chiffrement par flot

S’inspire du masque jetable.

Idée : remplacer la source aléatoire du masque par un générateur de nombres pseudo-aléatoires bien choisi. La racine devient la clé.

Allons voir ENIGMA avec ce point de vue.

L'ère des machines électromécaniques

Machines électromécaniques

Automatisation des opérations de chiffrement/ déchiffrement par des machines portatives.

Chiffrement polyalphabétique.

Utilisées tout au long du XXième siècle.

Machine de Hebern

Inventée en 1917

Rotor câblant une substitution monoalphabétique.

Le rotor est entraîné par engrenage lors de la frappe des touches.

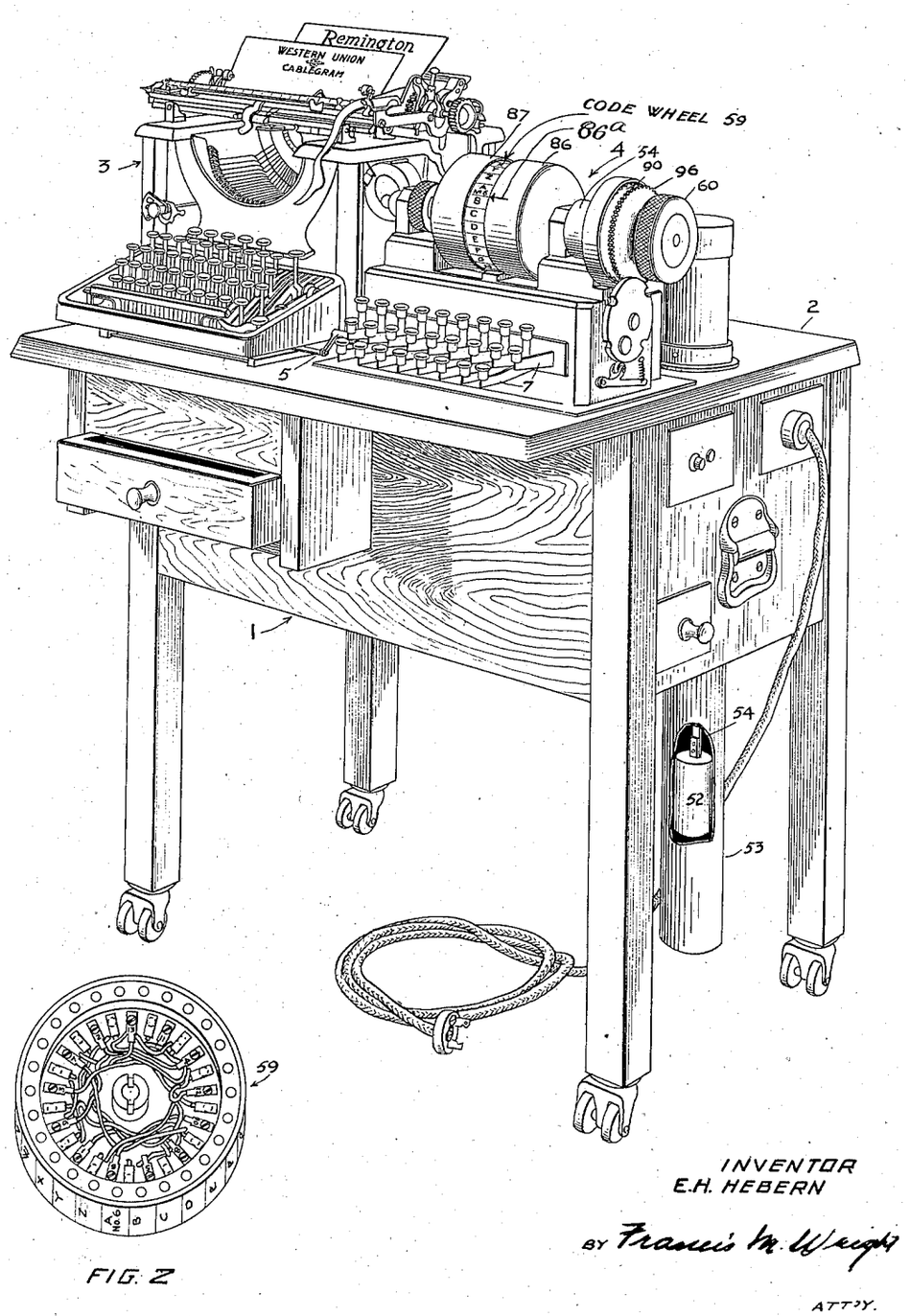
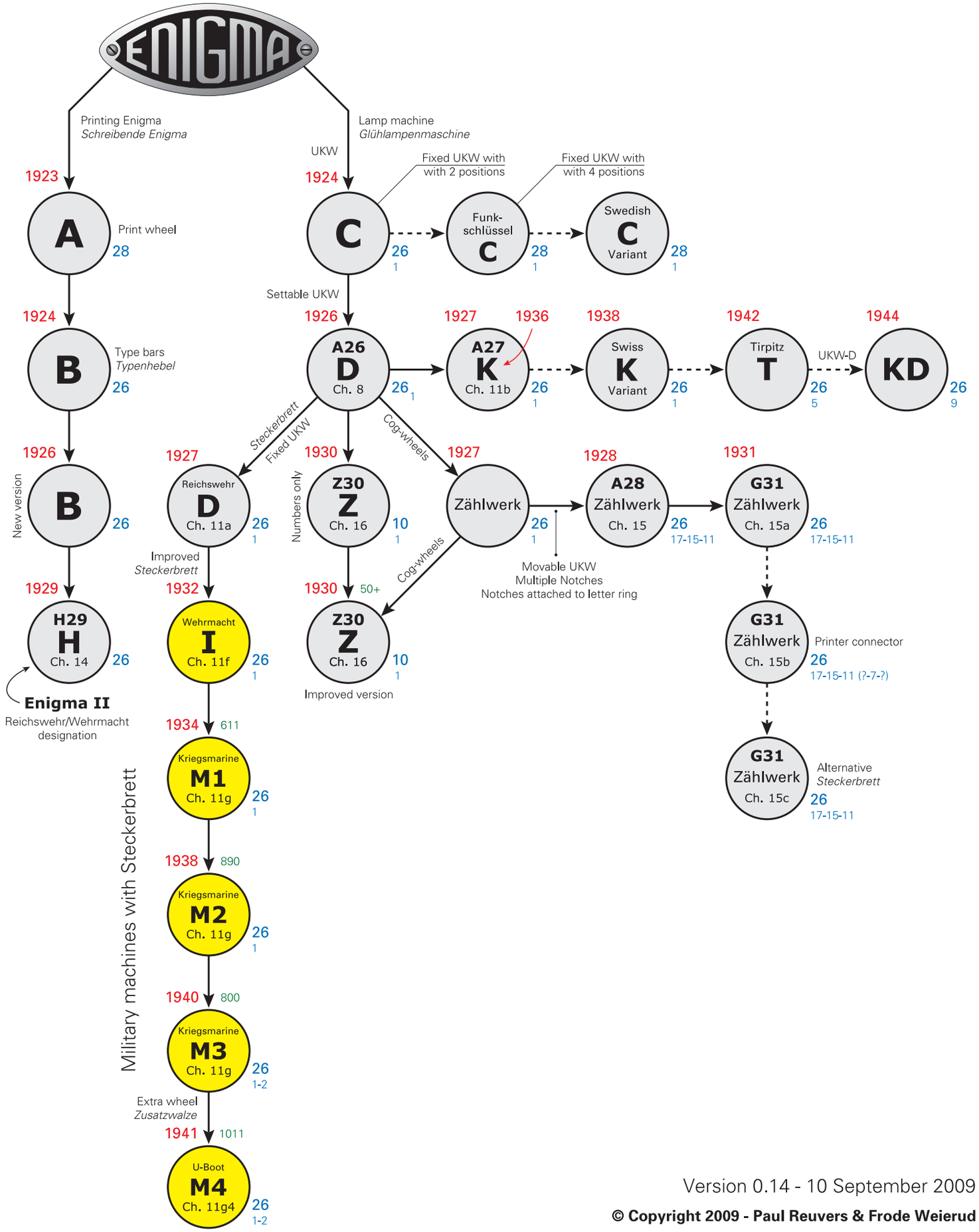


FIG. 2

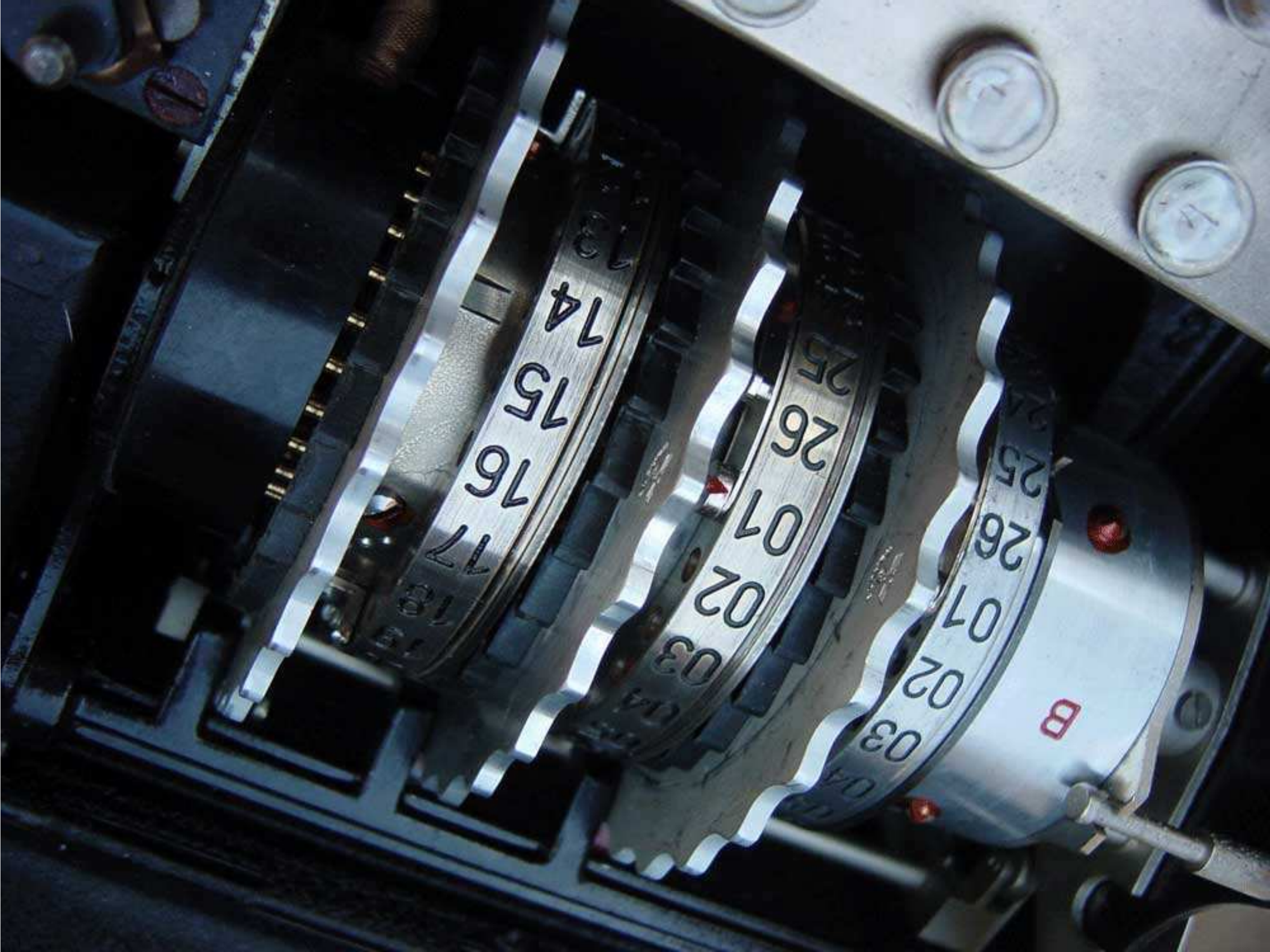

ENIGMA

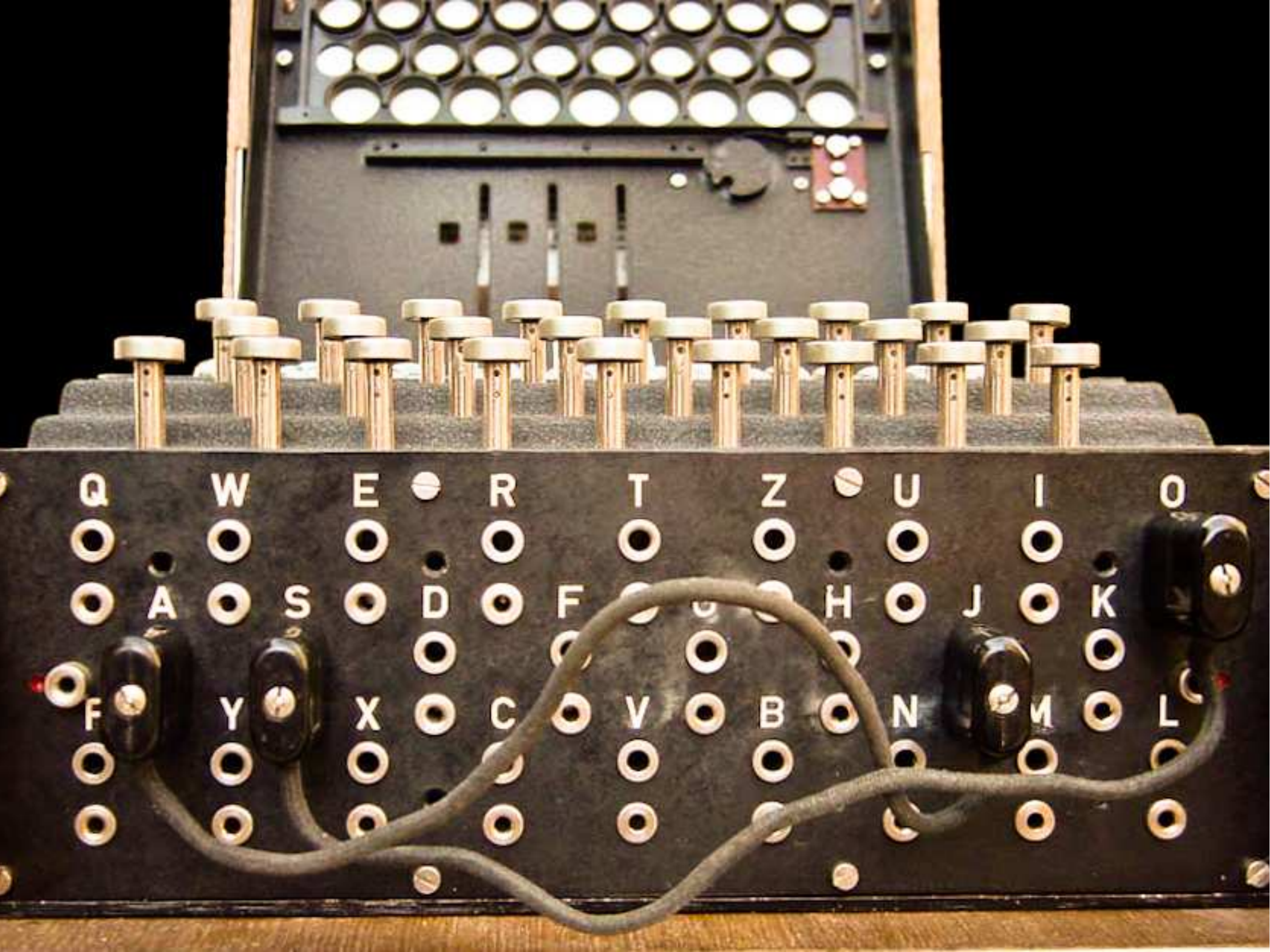


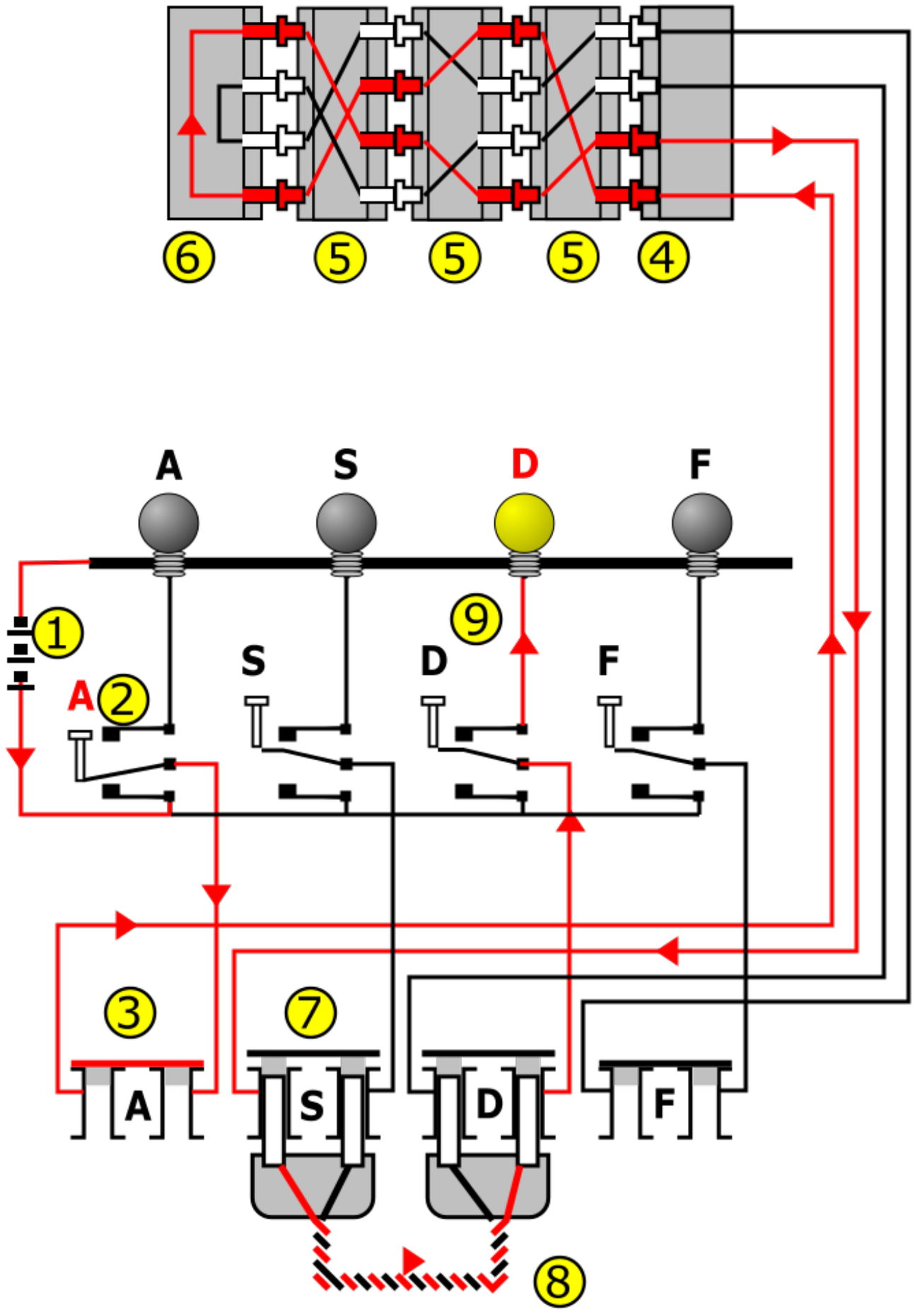
Version 0.14 - 10 September 2009


Zur Beachtung!
Beachte die Gebrauchsanleitung für die Chiffriermaschine (H. Dv. g. 13).
1. Zur Säuberung der Walzenkontakte alle Walzen mehrmals gegenseitig vor- und rückwärts drehen.
2. Zur Säuberung der Tastenkontakte sämtliche Tasten vor Einschaltung des Stromes mehrmals kräftig herunter drücken und hoch schnellen lassen, wobei eine Taste dauernd gedrückt bleibt.
3. Bei Einstellung der in den Fenstern sichtbaren Zeichen beachten, daß die Walzen richtig gerastet sind.
4. Die unverwechselbaren doppelpoligen Stecker sind bis zum Anschlag in ihre Buchsenpaare einzuführen. Die vordere Holzklappe ist danach zu schließen, da sonst 3 Lampen zugleich aufleuchten können.
5. Leuchtet bei Tastendruck keine Lampe auf, so sind die Batterie, ihre Kontaktfedern, ihre Anschlüsse am Umschalter und der Umschalter zu prüfen.
6. Leuchten bei Tastendruck eine oder mehrere Lampen nicht auf, so sind die entsprechenden Lampen, die Kontakte unter ihnen, die Kabel der doppelpoligen Stecker, die Steckerbuchsen einschließlich ihrer Kurzschlußbleche, die Walzenkontakte, die Arbeitskontakte unter den jeweils gedrückten Tasten und die Ruhekontakte unter den mit ihnen korrespondierenden Tasten zu prüfen und bei etwa vorhandenen Verschmutzungen und Oxydationen zu säubern. (Siehe auch Ziffer 2.)
Von Maschine Nr. A 4388 ab dient zur Lampenprüfung die Öffnung auf der rechten Lampenfeldseite.
Von Maschine Nr. A 4388 ab dienen zur Kabelprüfung die äußerste linke und rechte Buchse der mittleren Reihe am Steckerbrett und die Kabelprüflampe auf der linken Lampenfeldseite.
7. Walzenachse und Walzenbuchsen sind sauber zu halten und wie alle übrigen Lagerstellen hin und wieder mit harz- und säurefreiem Öl leicht einzufetten. Die festen Kontakte der Walzen sind alle 6—8 Wochen mit Polierpapier über zu schleifen und mit einem wenig getränkten Ollappen abzureiben. Die Tastenkontakte, die Lampenkontakte und die Kurzschlußbleche sind vor Öl zu schützen.
8. Schlüsseleingaben erfolgen entweder durch Zahlen oder Buchstaben.
Zum Umsetzen der Zahlen in Buchstaben oder umgekehrt dient nachstehende Tafel:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Dies ist ein geheimer Gegenstand im Sinne des § 88 des Reichsstrafgesetzbuches (Fassung vom 24. April 1934). Mißbrauch wird nach den Bestimmungen
A 5486
1936
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L


Nur Glühlampen mit 12 mm Durchmesser verwenden


13
14
15
16
17
25
26
01
02
03
25
26
01
02
03
B


Q W E R T Z U I O
A S D F H J K
F Y X C V B N M L


6
5
5
5
4
A
S
D
F
1
A
2
S
D
9
F
3
7
A
S
D
F
8

Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

Nr. 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SE	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	WD	YZ	OF	XK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
St	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WG	ZL	IV	JA	lsd	nuo	vcr	vcx
St	22.	I	II	IV	01	25	02	PZ	SE	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KF	NZ	IL	WM	BD	UO	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TF	RQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	II	07	05	23	ZX	EU	AC	GD	KP	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	OM	RL	DB	ST	AQ	PZ	XH	YN	IJ	oxd	lnb	ieu	ytt
St	17.	IV	I	II	12	08	21	ME	HX	BF	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VJ	YN	EL	pzg	evw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	UA	RX	PN	IS	WB	MH	ZV	bhe	xzm	yzk	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	UY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	II	V	03	25	10	CX	KN	JR	DQ	IU	TL	HZ	MF	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	FK	PS	CM	upc	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YM	WT	DE	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NP	FO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IR	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lro	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PI	CU	QA	OD	NM	aty	mbb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GP	LF	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	IV	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	PG	CO	FW	HJ	RY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	23	04	DY	CP	WN	OV	QH	UZ	RA	TI	GL	SM	hjy	nkt	ytn	pvc
St	2.	I	III	V	13	18	01	DR	VJ	FS	ZK	IU	HX	AQ	GT	YO	FC	qpq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	bol	ooi	ywv	sfb

Utilisation de la machine jusqu'en avril 1940

Préparation interne avec la clé du jour :

1. Ordonner les rotors et décaler les bagues
2. Câbler la permutation des entrées

Pour émettre un message :

1. Placer les rotors dans une position du jour
2. Choisir une position des rotors pour ce message et la chiffrer deux fois
3. Placer les rotors dans la position du message
4. Chiffrer le message

Machines Hagelin

Machines suédoises utilisées par l'armée française en 1940.

Ici une C-36 à 5 rotors.

KL-7

Machine à rotors utilisée par la NSA et l'OTAN de 1950 jusqu'aux années 70.

8 rotors, mouvements complexes.