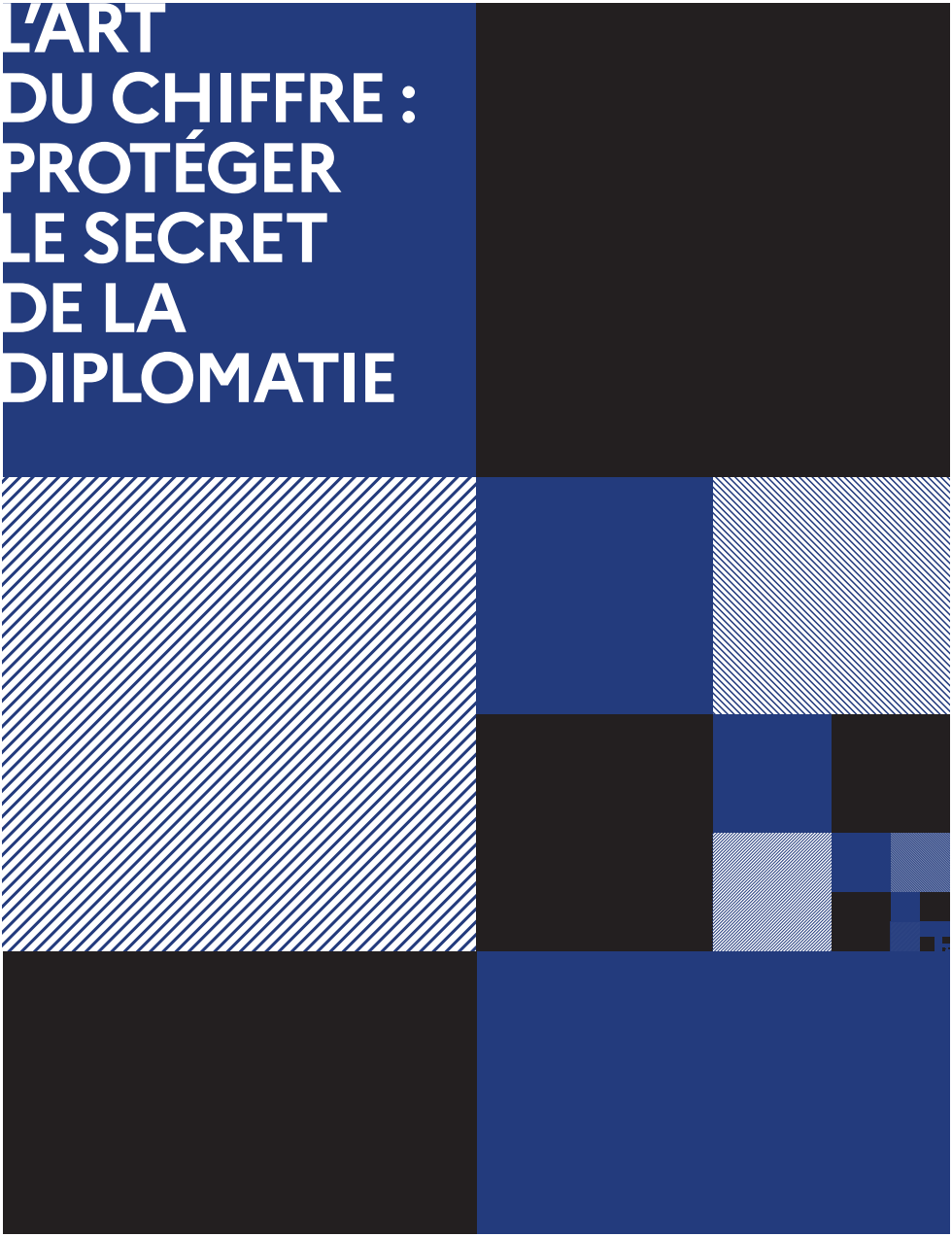
MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Liberté
Égalité
Fraternité

L'ART DU CHIFFRE : PROTÉGER LE SECRET DE LA DIPLOMATIE



L'ART DU CHIFFRE : PROTÉGER LE SECRET DE LA DIPLOMATIE

Conception
© MEAE – septembre 2023.
Direction de la communication et de la presse

Photos
© Judith Litvine
© Direction des archives diplomatiques

Sources
Archives diplomatiques françaises, Éditions de La Martinière, 2019
Direction des archives diplomatiques et Direction du numérique
du ministère de l'Europe et des Affaires étrangères.

Le besoin des hommes de communiquer est à l'origine de l'écriture, mais la nécessité leur apparaît presque aussitôt de préserver le secret de cette écriture, en dissimulant le sens des messages grâce à diverses techniques.

Afin de garantir le secret des informations qui circulent entre les diplomates en poste à l'étranger et le ministère des Affaires étrangères, les correspondances les plus sensibles sont longtemps restées chiffrées.

Le chiffrement consiste à coder le contenu d'un message afin que seul le destinataire puisse en prendre connaissance.

Cette exposition présente l'évolution des méthodes et techniques de chiffrement à travers l'histoire.

Bienvenue dans l'art du chiffre !

LES ORIGINES

Les premières méthodes de chiffrement remontent à l'Antiquité. Dès le Ve siècle avant JC, les chefs militaires grecs dissimulent le contenu de leurs communications en inscrivant leurs messages sur des tablettes de bois recouvertes de cire ou directement sur le crâne de leurs messagers. Cette technique, nommée **stéganographie**, atteint rapidement ses limites, car si le message est découvert par l'ennemi, il est immédiatement lisible.

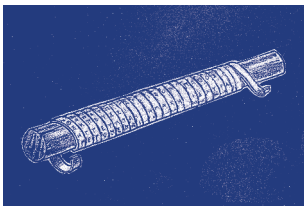
Pour contourner cet écueil, la **cryptologie** se développe. Ce procédé rend le message incompréhensible aux non-initiés. On distingue deux techniques de chiffrement :

— la **transposition** consiste à modifier l'ordre des lettres selon un code partagé par l'expéditeur et le destinataire. Par exemple, la scytale spartiate, autrement appelée le bâton de Plutarque, consistait à enrouler une bande de cuir remplie de lettres dans le désordre autour d'un bâton. Le message ne devenait lisible qu'enroulé autour du bâton du bon diamètre.

— la **substitution** consiste à remplacer une lettre par un autre élément. L'alphabet de César en est un bon exemple. Il consiste à remplacer chaque lettre par celle qui se trouve trois rangs après dans l'alphabet.

Dès le IIe siècle av. JC les fondements du chiffre moderne sont posés.

Stéganographie
Herodote témoigne de cette technique consistant à dissimuler un message tatoué sur le crâne d'un esclave.

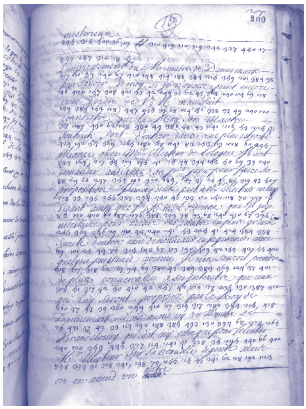


Scytale spartiate
Bâton de bois enroulé d'une bande de cuir pour lire ou écrire une dépêche chiffrée.

LA NAISSANCE DU CHIFFRE FRANÇAIS

L'histoire du chiffre français commence au XVI^e siècle, alors que les rois de France s'entourent de secrétaires cryptanalystes. Un des plus connus est François Viete, qui, sous Henri III et Henri IV, décrypte le système de chiffrement homophone espagnol où certains couples de lettres désignaient des mots (par exemple, LO signifiait Espagne).

Le XVII^e est marqué par la prouesse d'Antoine Rossignol, jeune mathématicien, qui offre la victoire à l'armée de Louis XIII en déchiffrant un message intercepté lors du siège d'une ville tenue par les huguenots. Richelieu comprend alors l'importance du chiffrement dans les activités diplomatiques et d'espionnage. Antoine Rossignol, puis son fils et son petit-fils, se mettent au service de Louis XIII puis de Louis XIV en élaborant le « Grand chiffre de Louis XIV », code constitué de 587 nombres différents alors réputé incassable. La famille Rossignol invente **les tables à chiffrer et les tables à déchiffre**r.



Grand chiffre de Louis XIV

Extrait d'un volume de correspondances avec Cologne. Dans cette lettre, en partie chiffrée et déchiffrée, le représentant de la France encourage une alliance avec le Danemark (1683).

LES DÉBUTS DU CHIFFRE AU MINISTÈRE DES AFFAIRES ÉTRANGÈRES

C'est en 1749 qu'est créé le premier bureau du chiffre du ministère des Affaires étrangères, auquel est confié le soin de protéger la correspondance politique.
À cette époque, les « cabinets noirs » s'activent partout en Europe et essaient de décrypter les correspondances chiffrées interceptées. Les périodes révolutionnaire et napoléonienne marquent une pause provisoire dans le développement du chiffre en France.

Le **télégraphe électrique**, inventé par Samuel Morse en 1844, accélère l'évolution technologique, qui va se poursuivre jusqu'à nos jours.
En 1874, le code Baudot (ou code télégraphique) est créé.
Il est l'un des premiers codes de télécommunication binaire issu d'une machine (le télégraphe), qui utilise 5 bits par caractères et 2 jeux de caractères.

À partir de 1900, tout se précipite, c'est le déferlement des techniques mécanique, électromécanique, électronique, informatique. Le **télégramme** devient le véhicule privilégié des communications diplomatiques. La brièveté nécessaire au langage télégraphique n'exclut nullement le sens des nuances.

En 1918 est créé le corps de chiffreurs des Affaires étrangères.
En 1948, c'est la fin du chiffrement manuel au Quai d'Orsay.

1981
Service du chiffre au ministère
de l'Europe et des Affaires étrangères.

L'ÉVOLUTION DES MÉTHODES DE CHIFFREMENT

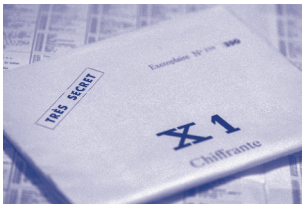
En 1949, le ministre des Affaires étrangères Robert Schuman lance les **télétypes chiffreurs**, machines Siemens à rotors reposant sur une clé mathématique. Entre 1949 et 1953, le Quai d'Orsay passe à la technique de **chiffrement mécanique**.
Les expérimentations débutent avec l'emploi de machines B-211 Hagelin, mises au point dans les années 1930 ; leur fonctionnement basé sur un mécanisme de rotors, comme les machines allemandes Enigma, assure une sécurité accrue des communications. Cependant, leur fragilité et le gain de temps négligeable par rapport à l'ancien système poussent à se tourner vers d'autres machines, dont l'utilisation s'avère une nouvelle fois peu concluante et apparaît somme toute peu sécurisée avec l'avènement du calcul par ordinateur.

En 1954, c'est le début du **chiffrement électronique aléatoire**.

Jusque dans les années 1960, le système Pénélope, utilisé par l'Otan, basé notamment sur l'emploi d'une règle de chiffrement manuelle, la CSP-1756, permet de ne chiffrer que les éléments clés d'un message : des lieux ou des dates, par exemple – le système est déclassifié en 1980. Aujourd'hui, les ordinateurs ont pris le relais.

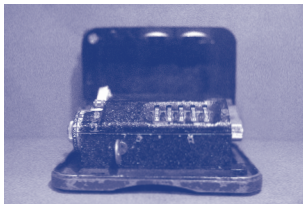
En 1990, les correspondances diplomatiques commencent à s'échanger par internet.

Le chiffre a officiellement disparu du ministère en 1998 avec la transformation de « la Direction du chiffre, de l'équipement et des communications » en « Service des systèmes d'information et de communication ».



Tables de chiffrement et de déchiffrement X1
Utilisées jusqu'en 1939.

B – 211
Machine à chiffrer de marque suédoise
Équivalent de la machine à chiffrer allemande Enigma, elle est utilisée par l'armée française pendant la Seconde Guerre mondiale entre 1939 et 1940, puis de 1945 à 1956.



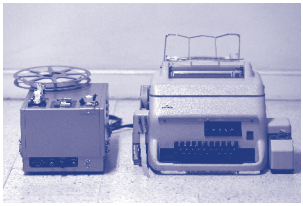
B – 36
Machine à chiffrer de marque suédoise
De type portable, elle est utilisée sur le front de 1939 à mai 1940.

Désormais, c'est la Direction du numérique qui est chargée de déployer les outils de communication classifiés (téléphone-visio Osiris, ou réseau intranet interministériel Isis) et d'assurer l'intégrité du système d'information du ministère (infrastructures et réseaux de communication permettant le chiffrement des données échangées).

Aujourd'hui, les chiffreurs sont, à proprement parler, des boîtiers de chiffrement qui permettent de sécuriser les échanges entre les quelque 300 implantations françaises à l'étranger et les *data centers* parisiens et nantais. Fournis par un constructeur français, ces équipements rendent, pour toutes personnes extérieures au ministère, les échanges indéchiffrables.

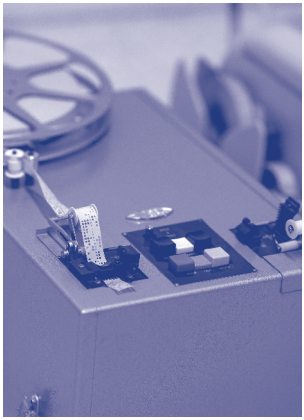
En 2023, on utilise le terme de chiffre pour désigner la protection de l'information (chiffrement des courriels pour les sécuriser, chiffrement des données qui circulent, via les logiciels et notre système de correspondance diplomatique : l'application Diplomatie).

Aujourd'hui, il existe différents « métiers du chiffre » (l'expression encore utilisée à l'oral est une réminiscence de ce riche passé) qui ont en commun de permettre aux agents du ministère de communiquer entre eux de manière sécurisée.



T100
Siemens

Télex (téléscripteur) entièrement électromécanique, utilisé de 1958 à 1990. Il fonctionnait avec des bandes perforées. Associé à un boîtier de chiffrement et de déchiffrement (Segma 31), cet outil permettait de saisir, de protéger et d'imprimer les correspondances.



Segma 31
Sagem

Mélangeur de bande permettant le chiffrement ou le déchiffrement d'un télégramme, utilisé du milieu des années 1950 au milieu des années 1990. Appareil couplé avec un télescripteur (T100).

TM30
Sagem

Télex chiffrant équipé d'un processeur Motorola 6800 et d'une carte électronique de chiffrement interne. Utilisé de 1985 à la fin des années 1990.

Son traitement de texte rudimentaire et sa mémoire de 10 000 caractères permettaient la rédaction de 4 pages en caractères Baudot (un des premiers codes de télécommunication binaire issu d'une machine comme le télégraphe, qui utilise 5 bits par caractères).

JEU

Saurez-vous décoder ce message en utilisant
le chiffre de César ?

Ce code consiste à remplacer la lettre du message clair
par la lettre se trouvant trois positions plus loin.

Par exemple,
la lettre A est remplacée par D,
la lettre B est remplacée par E, etc.

Lettres en clair	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
Lettres chiffrées	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Le message à décoder	OHV FDURWWHV VRQW FXLWHV
Votre décodage	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Réponse
↓

Les carottes sont cuites

Célèbre message codé diffusé
à Radio Londres, annonçant
l'imminence du débarquement
de Normandie.

↓