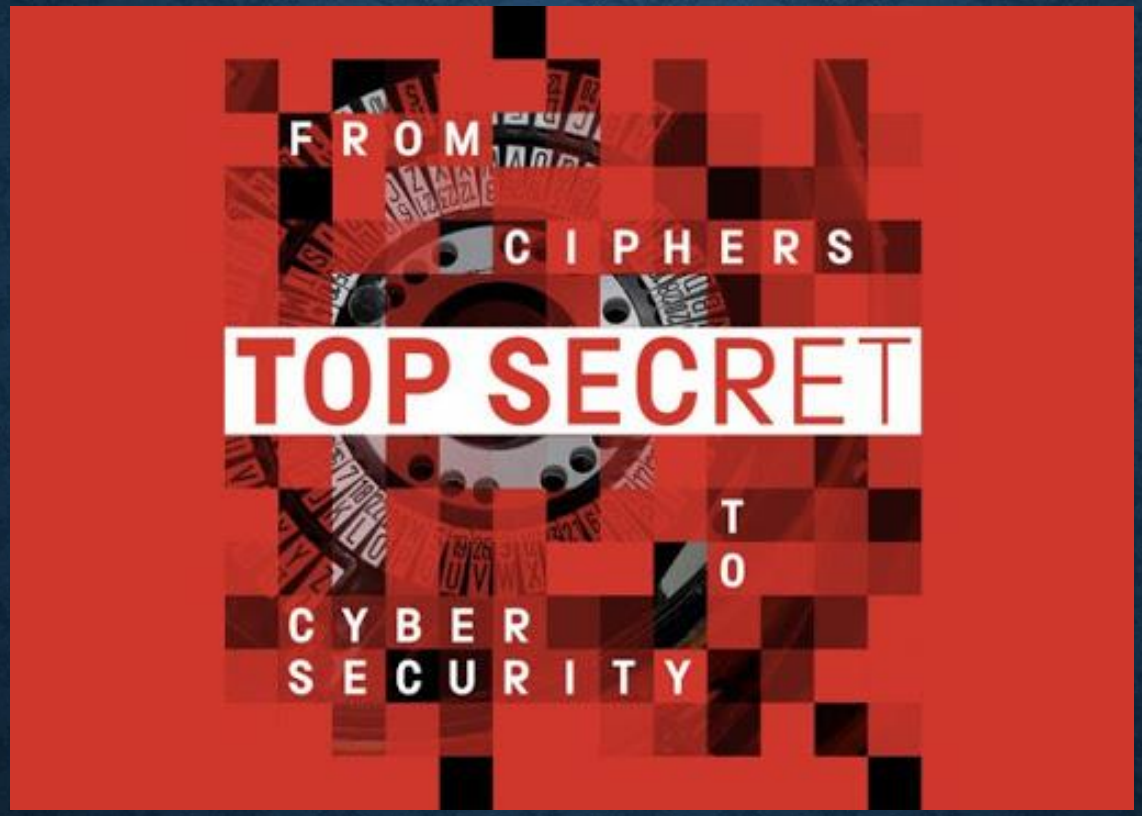
# EXPOSITION « *TOP SECRET* »




## Science Museum, London

10 juillet 2019 – 23 février 2020

Présentation réalisée par Florian Brunet pour l'ARCSI

# INTRODUCTION

***Government Communications HeadQuarters*** **(GCHQ)** (littéralement « Quartier Général des Communications du Gouvernement ») est un terme inventé en 1939 pour servir de couverture à la ***Government Code and Cypher School (GC&CS)***, qui était le Service de Cryptographie du Gouvernement Britannique depuis 1919.

# SOMMAIRE

# EVOLUTION HISTORIQUE

**- 405 av J-C** : Dans l'Antiquité grecque le général Lysander de Sparte utilise des messages secrets sur parchemins.

**- 850** : L'école arabe et le mathématicien « al-Kindi » décrivent une méthode pour décrypter les messages chiffrés.

**- 1655** : Après la guerre civile anglaise le maître de poste de Cromwell cherchait à intercepter les lettres pour informer le gouvernement.

**- 1900 – 1990** : Les Anglais utilisent les engrenages mécaniques et machines de chiffrement à rotor.

**- 50 av J-C** : Chez les Romains on utilise le chiffre de César qui substitue une lettre par une autre.

**- 1585** : Le gouvernement anglais déchiffre un message de la reine d'Ecosse « Mary » qui utilise un code secret pour transmettre les plans d'assassinat.

**- 1844 :** Espionnage du gouvernement anglais qui déchiffre les messages d'un Londonien révolutionnaire « Giuseppe Mazzini ».

# EVOLUTION HISTORIQUE

**- 1914-1918 :** La première guerre mondiale fait prendre conscience à l'Angleterre que sécuriser les communications sauve des vies.

**- 1916 :** Pendant la bataille de la Somme, les Allemands interceptent les plans des Anglais, ce qui explique en partie le nombre de morts côté alliés : 442 000 morts.

**- 1919** : Création de l'Ecole gouvernementale GC&CS (Government Code & Cypher School) devenue plus tard le Siège des Communications Gouvernementales. (CGHQ)

**- 1916 :** Pour sécuriser les communications, le GCHQ met en place le Fullerphone à la place du Trench phone.

**- 1917** : Les briseurs de code britanniques ont intercepté des télégrammes d'origine allemande. Les révélations ont contribué à l'entrée des USA dans la guerre.

**-1923 :** Les Allemands commercialisent Enigma une machine électromécanique portable servant au chiffrement de l'information. Ils créent en parallèle une version plus développée dédiée aux militaires.

# EVOLUTION HISTORIQUE

- **1940 – 1980 :** Les Anglais multiplient les partenariats entre le monde de l'industrie et les services publiques. Chaque agence gouvernementale a une machine dédiée.

- **1962 :** Le centre du GCHQ de Scarborough donne des informations vitales sur l'arme nucléaire soviétique.

- **1939 :** le CGHQ déménage à Bletchley Park pour déchiffrer les communications des Italiens, Allemands et plus tard des Japonais. Bletchley Park devient le centre de cryptanalyse en temps de guerre.

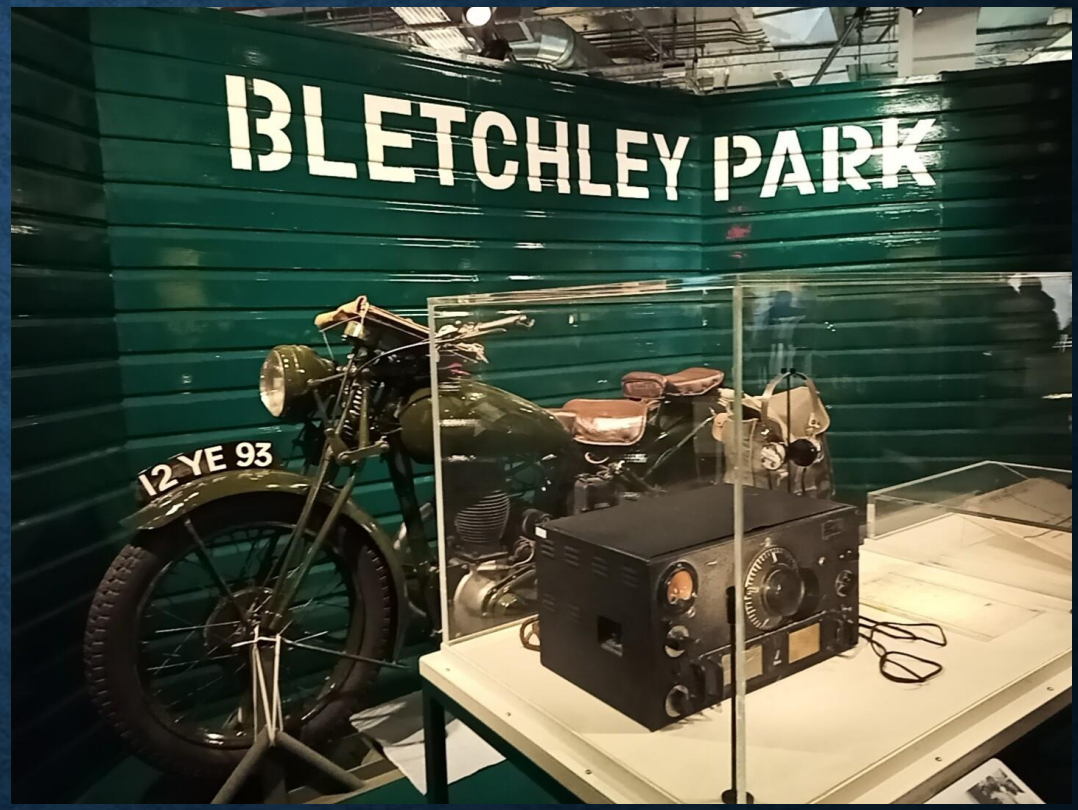
- **1940 – aujourd'hui :** Le GCHQ et l'Ecole du Chiffre sécurisent les téléphones des leaders anglais.

- **1988 :** Au début d'internet le GCHQ expérimente des programmes de recherche sur le développement des virus/worms.

# BLETCHLEY PARK

Le système était déjà en place avant la seconde guerre mondiale (1939-1945)

- Les « Red Forms » interceptaient les messages.
- Les Y stations traitaient les messages.
- La vitesse était vitale.



# BLETCHLEY PARK

Depuis les Y stations ils utilisaient des motos pour envoyer des messages à Bletchley Park.

Environ 400 motos faisaient le chemin chaque jour.

Des milliers de messages déchiffrés chaque jour.

Partager des messages
(1915)

# BLETCHLEY PARK

**Message chiffré avec Lorenz.**

**Message chiffré avec Enigma.**

**Les mathématiciens calculent les paramètres de Lorenz à la main.**

**Les membres de la Royal Navy utilisent « The Colossus Machine » pour déchiffrer les paramètres de Lorenz de façon électronique.**

**Stockage des informations.**

**Les traducteurs traduisent le texte en Anglais.**

**Les déchiffreurs utilisent les paramètres trouvés par « The Bombe » pour déchiffrer tous les messages.**

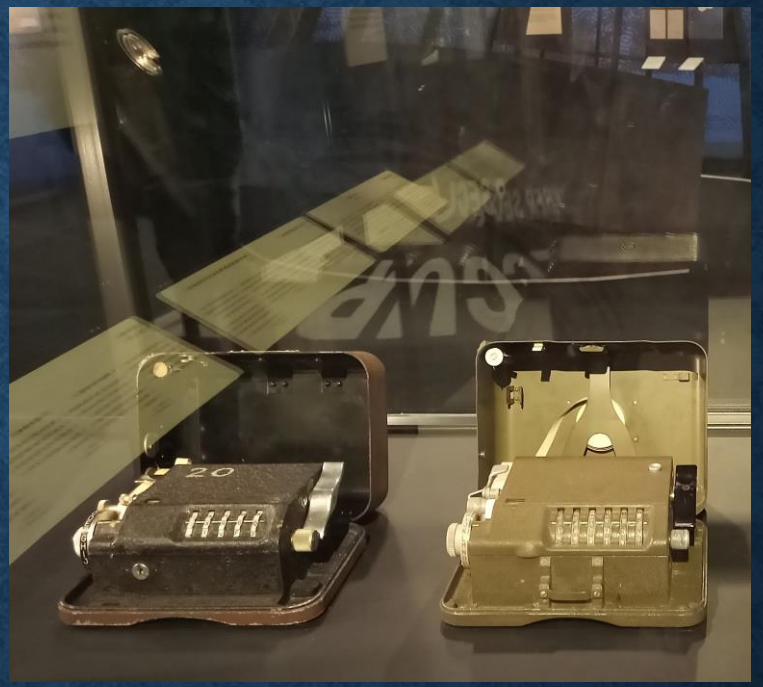
**Si « The Bombe » ne donne pas de résultat ils font le calcul à la main.**

**L'équipe de femmes de la Royal Navy configure « The Bombe » pour essayer de bruteforcer chaque combinaison**

**Les mathématiciens reçoivent les messages de Enigma et préparent les instructions**

# **Les machines servant au chiffrement** (1800-1940)

Chiffrement par Cylindre
(1800-1900)



Machine à chiffrer portable Hagelin C-36
(1936)

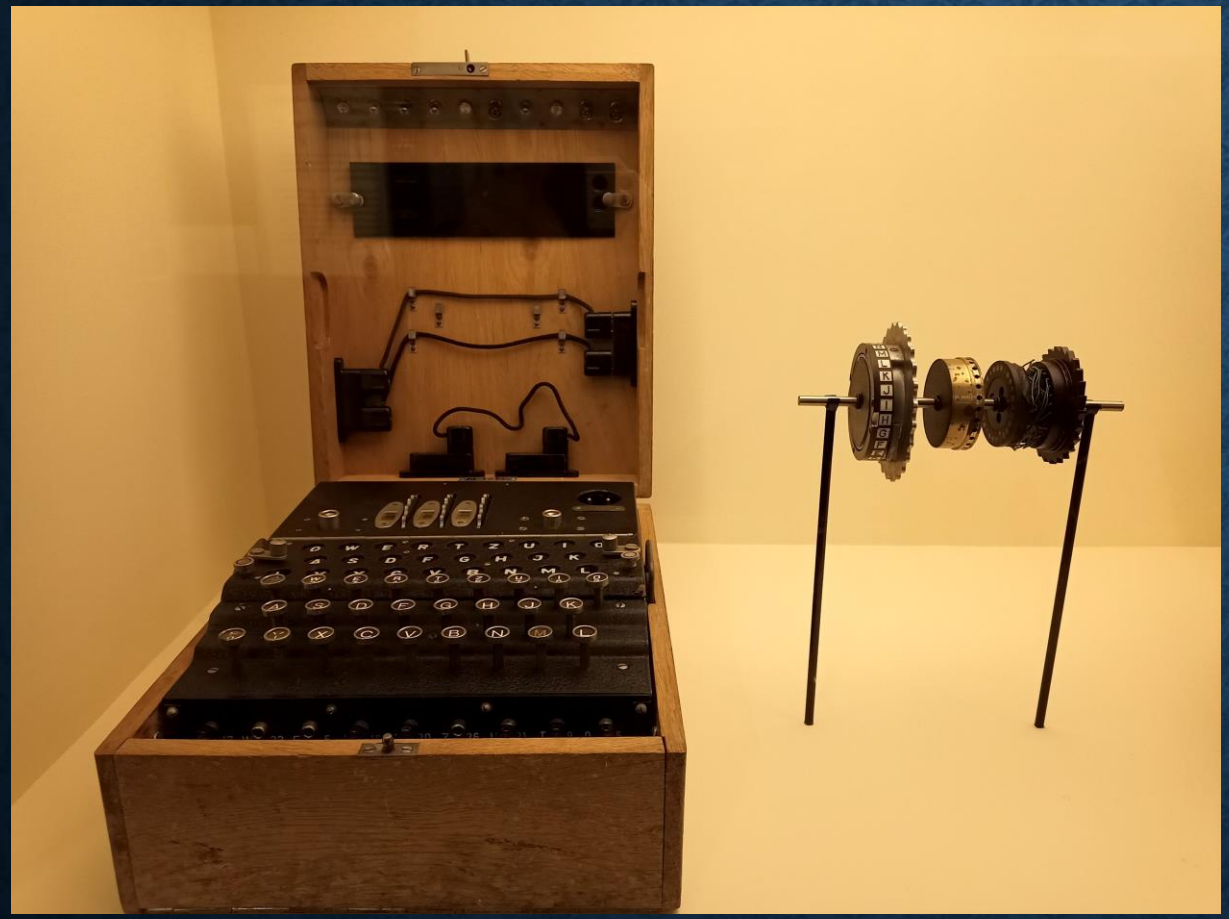
Machine à chiffrer portable US army M-209B
(1940)

# **Les téléphones pendant la guerre** (1914-1918)

Trench phone
(1914-1918)


FullerPhone
(1916-1918)

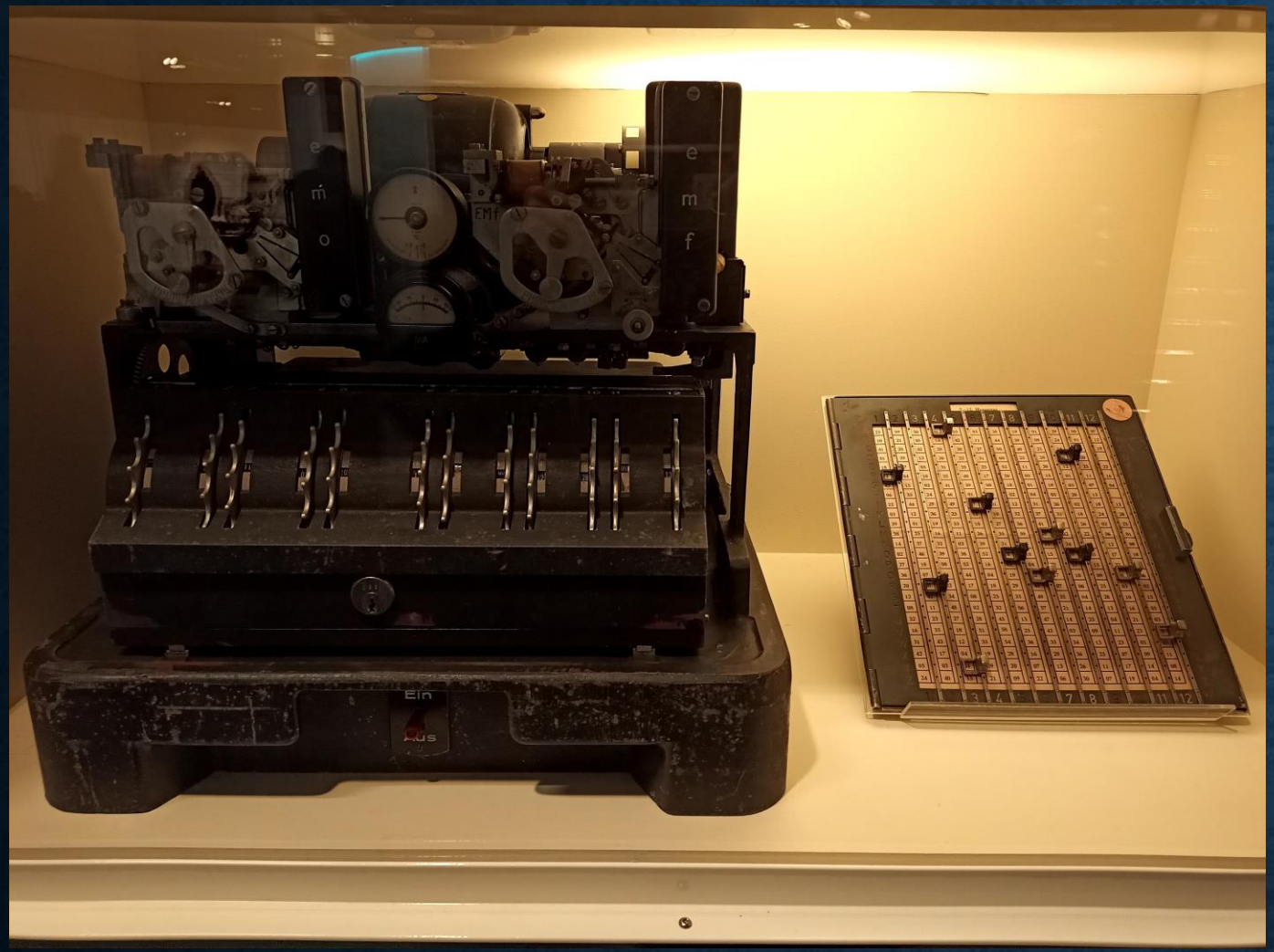
# **Les machines servant au chiffrement** (1938-1944)



Machine Enigma
(1940)

Copie Machine Enigma pour étude
(1940)

# **Les machines servant au chiffrement** (1938-1944)



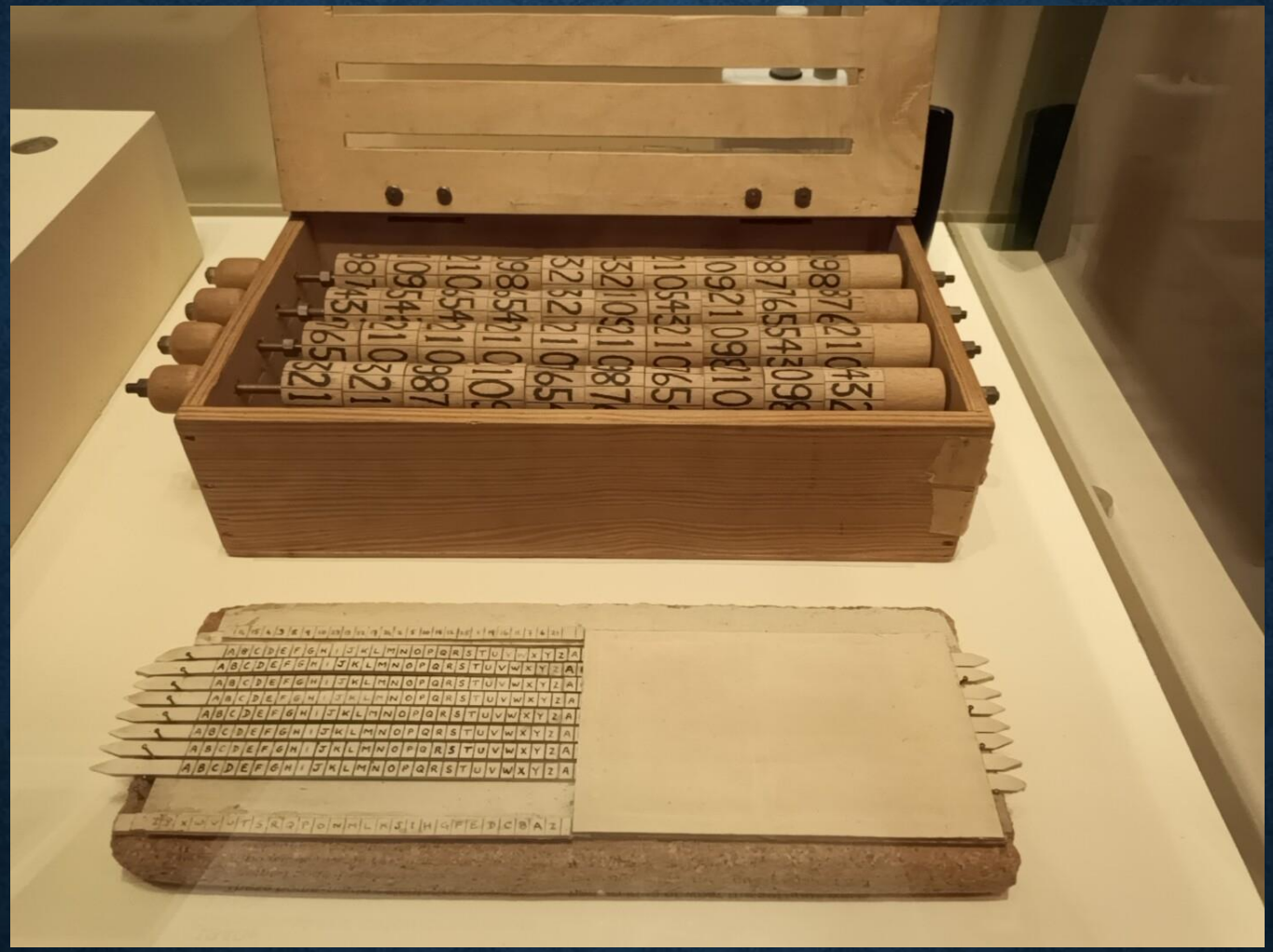

Machine Lorenz
(1940)


Le SG41 est la machine sans faille
(Allemagne, 1944)

# **Les machines servant au chiffrement** (1938-1944)

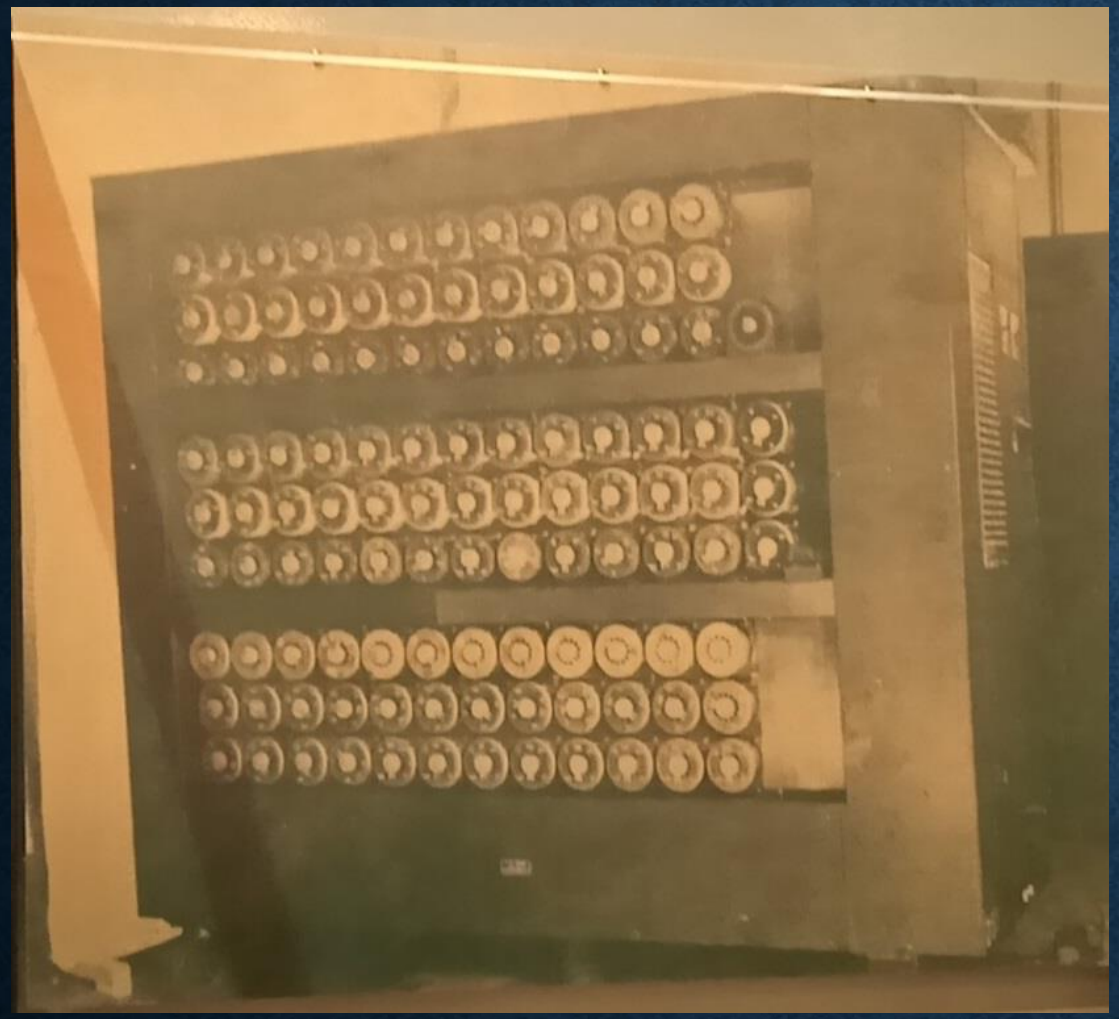
Typex machine
(Angleterre, 1938)

# **Les machines servant au déchiffrement** (1938-1945)



Une machine pour déchiffrer les messages de Enigma à la main (1940)

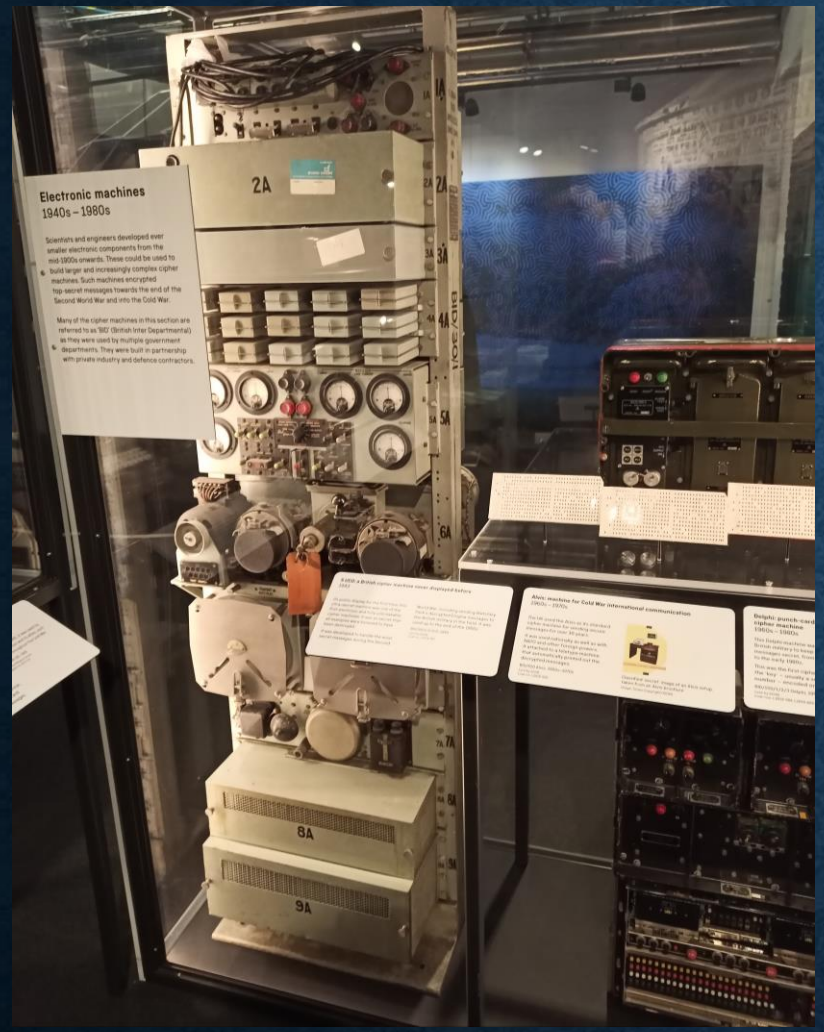
# **Les machines servant au déchiffrement** (1938-1945)



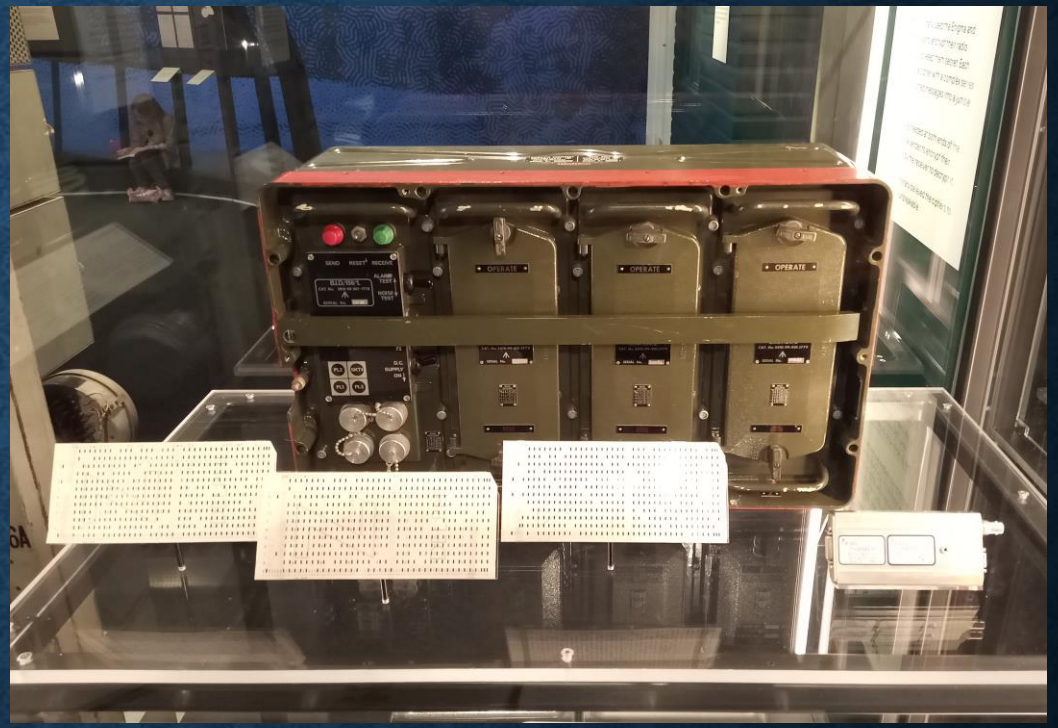
Bombe machine
(1938)

Rotor de la Bombe machine
(1938)

# **Les machines servant au chiffrement** (1943-aujourd'hui)

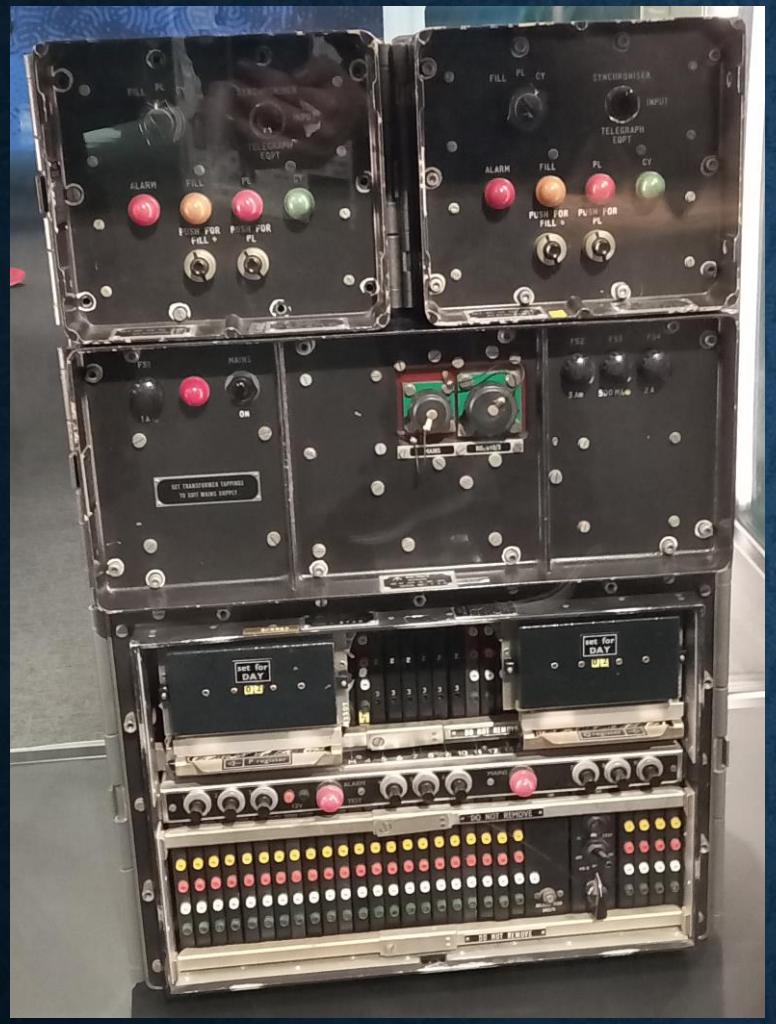



5 UCO
(1943)



Alvis
(1960-1970)

# **Les machines servant au chiffrement** (1943-aujourd'hui)




Delphi
(1960-1980)


Thamer (2000-2030)

Emetteur radio Iraquien
(2004)

# Les téléphones du gouvernement anglais


1


1

2

3

4

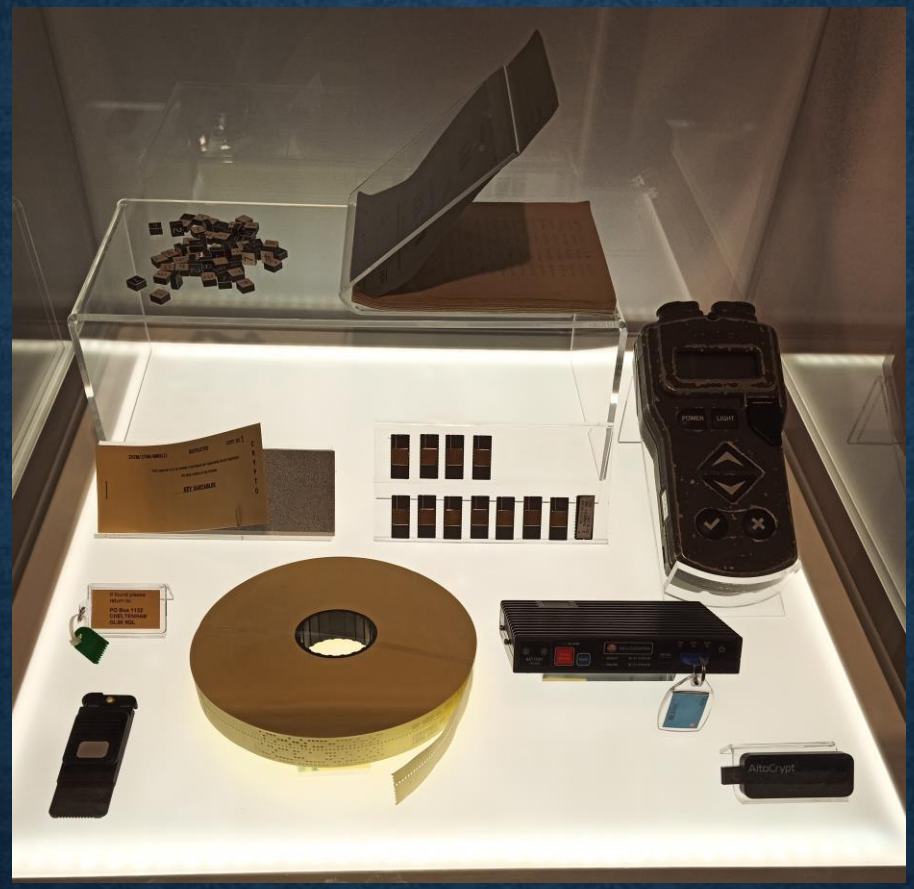
1- Téléphone utilisé par Winston Churchill (1941)
2- Téléphone rouge pendant la Guerre Froide (1960)
3- Téléphone des ministres anglais (1980)
4- Téléphone de la Reine d'Angleterre (1995)

# La stéganographie : des outils pour dissimuler de l'information

Microscope
(1961)


Microscope
(1961)

# Des outils pour générer des nombres aléatoires




Générer des nombres aléatoires
(1961,+∞)

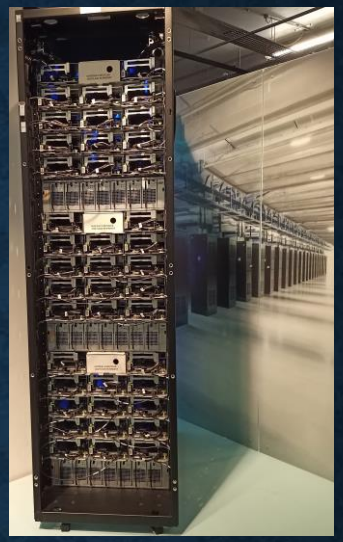
# Les affaires d'espionnage d'un autre temps…

Gordon Lonsdale, Arrestation pour espionnage
(1961)


Révélations de Zircon et GCHQ
(1987)

# Les défis d'aujourd'hui?


Data center
(2017)



Data center

Murmur study
(2010)

**Le problème n'est plus de diffuser l'information mais de la contrôler.**


Carte des cables sous-marins
(2020)

# CONCLUSION

Le temps évolue mais les problématiques restent.