1400

1462
Léon Battista Alberti [1404–1472] et son cadran chiffrant

Première substitution polyalphabétique

1518
Jean Trithème [1462–1516]

Premier ouvrage imprimé de cryptologie

1500

1552
Boîte à chiffrer de Henri II **[257]**

1558
Philibert Babou [vers 1500–1569]

Secrétaire et cryptologue de François I^er^

1563
Giovanni Battista Della Porta [1535–1615] et son cadran chiffrant

Première société savante sur la cryptologie

Vers 1570
Girolamo Cardano [1501–1576]

Mathématicien, inventeur du procédé cryptographique avec masque à trous

Traité de 1585
Blaise de Vigenère [1523–1596]

Inventeur d'un système de substitution polyalphabétique très robuste, synthèse de tous les apports de ses prédécesseurs mais complexe à mettre en œuvre sans instrument. Il sera utilisé de façon maladroite par Marie-Antoinette.

1587
Procès et décapitation de Marie Stuart, dont les lettres compromettantes avaient été décryptées.

1591
François Viète [1540–1603]

Premier cryptanalyste émérite connu

1600

1626–1628
Antoine Rossignol [1600–1682] et ses descendants **[258]**

Déchiffrement d'un message huguenot à Réamont en 1626, puis au siège de La Rochelle pour Richelieu en 1628.

1630
Cesare Ripa, [vers 1555–1562]

Réédition chez Donato Pasquardi de *Della piu che novissima Iconologia...* **[5]**

1630
François Leclerc du Tremblay, dit père Joseph **[32]** [1577–1638]

Lettre du consul Décury **[45]**

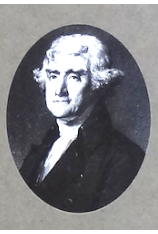
1700

1791
Tableau de chiffrement utilisé pour la correspondance avec Eugène de Beauharnais, lorsqu'il était vice-roi d'Italie. **[264]**

1793 *Le Cabinet noir* **[259]**
Procès et condamnation de Marie-Antoinette bien que le décryptement de ses lettres compromettantes n'ait pas été évoqué lors de son procès.

1794 Télégraphe optique de Claude Chappe **[279]**

1800



Vers 1800
Thomas Jefferson [1743–1826]

Cylindre de chiffrement polyalphabétique de Thomas Jefferson

1832
Invention du télégraphe électrique par Pavel Schilling

1844
Perfectionnement du télégraphe électrique par Samuel Morse (code universel)

1870
La défaite française est en partie imputable à un chiffre archaïque facilement percé par les Prussiens.

1876
Invention du téléphone par A. G. Bell

1883
Auguste Kerckhoffs [1835–1903]

Promoteur de la réglette de Saint-Cyr **[278]**

1891
Cylindre de chiffrement revu par Étienne Bazeries **[269]**

1900

1914

Bataille de Tannenberg : faute d'avoir reçu les documents du Chiffre, les généraux russes sont obligés de communiquer en clair par radio les ordres de mouvement aux unités, ce qui provoque leur déroute face aux Allemands.

1917

Gilbert Vernam [1890–1960]
Chiffrement pour télégraphe en 1917

Inventeur du système de chiffrement dit «à clé une fois» ou «à masque jetable» : clé aussi longue que le message à transmettre et à n'utiliser qu'une seule fois.

février 1918

Arthur Scherbius [1878–1929]
Brevet d'une machine électrique chiffrante à rotors (future Enigma utilisée par les Allemands), du 23 février 1918.

avril 1918

Capitaine Georges Jean Painvin **[284]** [1886–1980]
Il perce le secret du chiffre allemand durant la Première Guerre mondiale.

vers 1930

Marian Rejewski [1905–1980]
Mathématicien polonais, premier décrypteur d'Enigma et créateur des premières *bombas* permettant de retrouver les clés d'Enigma.

1934

C-36 **[288 bis]**
Machine à chiffrer développée avant la Seconde Guerre mondiale par la société A.B. Cryptoteknik du Suédois Boris Hagelin et utilisée par l'armée française.

38–40

Alan Turing [1912–1954]
Rôle majeur dans la cryptanalyse de la machine Enigma. Inventeur de la machine (théorique) qui porte son nom.

42–45

Bataille de l'Atlantique gagnée par les Alliés en grande partie grâce au décryptement de la machine Enigma. **[289]**.

1949

Claude Shannon [1916–2001]
Père fondateur de la théorie de l'information. Démontre en 1949, le caractère indécryptable du masque jetable à condition que la clé soit aléatoire.

1950–1970

Tarec (transmission automatique régénératrice et chiffrante) repose sur le principe de la clé à usage unique : l'émetteur et le destinataire du message à chiffrer possèdent tous deux un exemplaire d'une même bande perforée constituant la clé aléatoire. **[Palier]**

1952

CX-52 **[288]**.
Machine à rotors améliorée

1956 –1963

Myosotis, première machine française entièrement électronique **[293]**

1962

Crise des missiles de Cuba, dont une des conséquences a été la création d'une ligne de communication chiffrée entre Washington et Moscou : le fameux «téléphone rouge», **[Palier]** qui en réalité était un téléimprimeur chiffrant avec bandes aléatoires

1976

Whitfield Diffie [né en 1944] et Martin Hellman [né en 1946]
Concept de cryptographie à clé publique

1977

Mise en œuvre du concept de Diffie et Hellman par Rivest, Shamir et Adleman : fondé sur la difficulté de factoriser les nombres dès lors qu'ils sont très grands, le système RSA (initiales des auteurs) est aujourd'hui universellement utilisé dans la plupart des transactions électroniques.

1976

Avènement de la cryptologie asymétrique, qui repose sur l'utilisation d'une clé publique (diffusée) et d'une clé privée (gardée secrète), l'une permettant de chiffrer le message et l'autre de le déchiffrer. Combinée à des systèmes symétriques, elle a permis le développement d'une cryptologie de masse indispensable aux applications touchant un grand nombre d'utilisateurs.

2000

Teorem, de la société Thalès **[297]**
Téléphone portable de très haute sécurité chiffrant de bout en bout les communications des hauts responsables gouvernementaux et militaires. À comparer avec le système Sigsaly (plusieurs tonnes de matériel) utilisé par Roosevelt et Churchill pendant la Deuxième Guerre mondiale.

2013

Affaire Snowden : révélation de l'espionnage de masse par la NSA (National Security Agency) avec mise en place de portes dérobées dans les logiciels de cryptographie systématiquement soumis à son contrôle.