ISÈRE

INSTITUT FOURIER

Laboratoire de Mathématiques UMR 5582 CNRS-UJF

LABORATOIRE JEAN KUNTZMANN

Cryptologie

Histoire de la cryptographie

Léon Battista Alberti, grand philosophe et écrivain de la renaissance, publie De Componendis Cyphris, premier ouvrage occidental de cryptographie. Il invente le cadran chiffrant et, pour la première fois, propose un chiffre de substitution polyalphabétique

1467

Dans son Traicté des chiffres ou secretes manières d'escrire, Blaise de Vigenère publie la méthode de chiffrement de substitution polyalphabétique qui conservera son nom

1586

Arthur Scherbius développe la machine à chiffrer Enigma, qui sera utilisée par l'Allemagne nazie pendant la seconde guerre mondiale

1919

Joseph Mauborgne et Gilbert Vernam inventent le masque jetable système inconditionnellement sûr

1918

Stephen Wiesner jette les bases d'une cryptographie quantique en inventant le principe d'une monnaie quantique

1970

Horst Feistel développe le chiffre Lucifer chez IBM

1999

Le WEP est adopté pour le chiffrement des communications wifi

1976

1988

Charles Bennett et Gilles Brassard réalisent la première expérience de cryptographie quantique

2004

Le WPA2 est la nouvelle norme pour le chiffrement des communications wifi. Il pallie les faiblesses du WEP

Echange de clef de Diffie et Hellman

1984

Tahar Elgamal propose un cryptosystème fondé sur l'échange de clefs de Diffie-Hellman et le logarithme discret

2001

Nouveau standard de cryptographie, AES fondé sur l'algorithme Rijndael pour pallier les faiblesses de DES

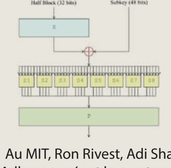
La machine de Lorenz est utilisée pour chiffrer les communications entre les hauts dirigeants allemands

1939

1945

Les Rossignol père et fils mettent au point le grand chiffre, au service de Louis XIV

17e siècle



Naissance de DES, premier standard de cryptographie, fondé sur Lucifer

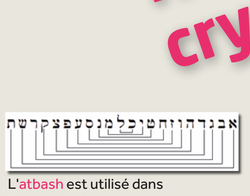
Au MIT, Ron Rivest, Adi Shamir et Leonard Adleman créent le cryptosystème RSA, algorithme de chiffrement à clef publique

1977

1991

Phil Zimmerman publie PGP, un logiciel ouvert de chiffrement grand public utilisant les meilleurs algorithmes

Ronald Rivest crée MD5, une fonction de hachage cryptographique encore très utilisée



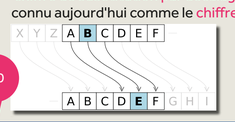
L'atbash est utilisé dans l'ancien testament, notamment le livre de Jérémie

-600

-404

Selon Plutarque, Lysandre de Sparte fait usage de la scytale, un chiffre de transposition

-50



César utilise plusieurs chiffres, dont un chiffre de substitution par décalage connu aujourd'hui comme le chiffre de César

-400

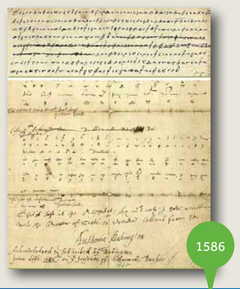
0

Une des plus anciennes descriptions connues de chiffre de substitution monoalphabétique se trouve dans le Kâmasûtra, qui recommandait aux femmes de chiffrer leur correspondance afin de cacher leurs liaisons

10e siècle

Le manuel du secrétaire, Adab-al-Kuttab contient une partie consacrée à la cryptographie

Les cryptanalyses célèbres

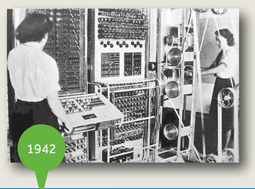


1586

Procès du Complot de Babington. Francis Walsingham, chef de l'espionnage anglais sous Elisabeth I parvient à décrypter les messages échangés entre Marie Stuart, reine d'Ecosse, et les comploteurs, prouvant ainsi sa culpabilité. Elle fut décapitée

1893

Etienne de Bazeries cryptanalyse le grand chiffre



1942

Le chiffrement de Lorenz est cassé par les cryptanalystes de Bletchley Park, avec l'aide du Colossus, le premier ordinateur électronique numérique

1918

Le lieutenant Georges Painvin casse le chiffre allemand ADFGVX et contribue ainsi à la victoire française

1996

Une faille est découverte dans MD5

2001

Scott Fluhrer, Itsik Mantin et Adi Shamir démontrent la faiblesse du WEP

9e siècle

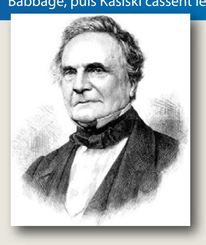
Al Kindi publie le premier ouvrage connu de cryptanalyse, Manuscrit sur le déchiffrement des messages cryptographiques, qui présente l'analyse des fréquences

0

1854

1863

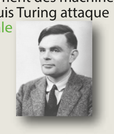
Babbage, puis Kasiski cassent le chiffre de Vigenère



1939

1945

Ian Turing et Dilly Knox améliorent le fonctionnement des machines polonaises, puis Turing attaque l'Enigma navale



1933

Les mathématiciens polonais Marian Rejewski, Jerzy Różycki et Henryk Zygalski attaquent avec succès une première version d'Enigma, et créent la première bombe cryptologique

1998

La Electronic Frontier Foundation casse DES par force brute en 2 jours

2010

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar et Vadim Makarov parviennent à craquer les détecteurs commerciaux utilisés pour la cryptographie quantique.

Contexte

-400 — Guerres entre les grecs et les perses

9e siècle — Apogée de la civilisation arabo-musulmane sous la dynastie des Abbassides

15e siècle — Renaissance en Europe

18e siècle — 19e siècle — Développement du télégraphe optique, puis électrique, puis sans fil (la TSF)

1914 1918 — Première Guerre mondiale

1939 — 1945 — Seconde Guerre mondiale

1947 — Invention du transistor

1953 — Premier ordinateur IBM

APPLICATIONS

Graphisme : Fanny BASTIEN (CNRS)