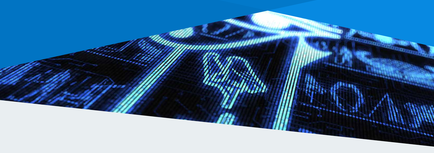
digicert®

LA CRYPTOGRAPHIE
À L'ÈRE DE L'INFORMATIQUE

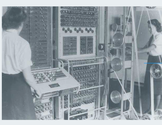


L'histoire de la cryptographie ressemble à un cycle sans fin où les nouveaux algorithmes finissent tôt ou tard par être déchiffrés. Prochaine grande étape : la cryptographie quantique, une nouvelle technologie de chiffrement entièrement basée sur les propriétés quantiques des photons polarisés.

1974

BLETCHLEY PARK

Lors de la déclassification des informations sur l'implication de Bletchley Park dans le craquage du code d'Enigma, la machine de chiffrement de l'armée allemande, le public prend conscience du rôle de l'informatique dans le cassage des codes.



1976

NIST

L'algorithme DES (Data Encryption Standard) est approuvé par le NIST et devient le standard de chiffrement mondial.

RSA

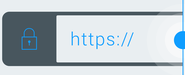
L'algorithme RSA est la première application de cryptographie à clé publique se servant d'une clé publique accessible à tous et d'une clé privée connue uniquement du destinataire pour déchiffrer un message.

1994

CLÉ DES

De nouveaux ordinateurs surpuissants peuvent déchiffrer les clés DES de 56 bits (2 puissance 56, soit environ 72 quadrillions de combinaisons possibles).

1996



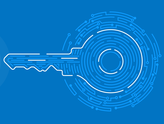
SSL

Netscape lance la version 3 de SSL (Secure Sockets Layer). Les certificats électroniques associés vérifient l'identité des serveurs et intègrent cette information dans Netscape Navigator.

1999

TLS

La version 1.0 de TLS (Transport Layer Security) succède au protocole SSL 3.0.



2005

ECC

La NSA lance la Suite B, une série d'algorithmes de cryptographie sur courbes elliptiques (ECC) destinée aux signatures numériques et aux échanges de clés.

2014

CHIFFREMENT 2048 BITS

Le NIST fixe une date limite pour la migration des certificats 1024 bits vers des certificats 2048 bits.

digicert®

DigiCert estime qu'il faudrait plusieurs quadrillions d'années aux technologies informatiques actuelles pour craquer une clé RSA de 2048 bits (estimation reprise dans le rapport de la National Academy).

2029

QUANTUM

Pour le NIST, un ordinateur quantique sera capable de casser cette même clé en quelques mois dans les 10 ans à venir, marquant ainsi l'avènement de l'ère de la cryptographie quantique.

digicert®

PRÊT POUR LE SAUT QUANTIQUE ?

L'informatique quantique promet de faire voler en éclats les standards actuels de chiffrement RSA/ECC. Ce n'est qu'une question de temps. Pour anticiper ce virage, consultez notre kit PQC (Post-Quantum Cryptography Toolkit).

DigiCert.com/PostQuantum