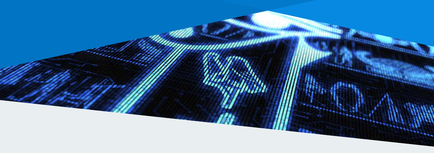
digicert®

KRYPTOGRAFIE
IM COMPUTERZEITALTER

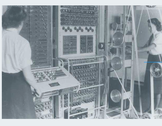


Die Geschichte der Kryptografie ist ein ständiger Wettlauf: Für jeden neuen Verschlüsselungsalgorithmus wird schon bald eine Entschlüsselungsmethode entwickelt. Die nächste Runde wird die Quantenkryptografie sein, bei der Informationen als Drehwinkel von Photonen verschlüsselt werden.

1974

BLETCHLEY PARK

Informationen zur Dechiffrierung der Enigma-Codes in Bletchley Park werden freigegeben und machen die Öffentlichkeit auf die Rolle von Computern beim Entschlüsseln von Codes aufmerksam.



1976

NIST

Die US-Behörde NBS (heute NIST) genehmigt den Data Encryption Standard (DES), der später weltweit zur Standard-Chiffre wird.

RSA

Mit der RSA-Chiffre werden erstmals öffentliche Schlüssel in der Kryptografie verwendet: Die Verschlüsselung erfolgt mit einem allgemein zugänglichen, öffentlichen Schlüssel, während zur Entschlüsselung ein privater Schlüssel verwendet wird, den nur der Empfänger besitzt.

1994

DES-SCHLÜSSEL

Mit modernen Computern können mit DES verschlüsselte Nachrichten (trotz der 2^{56}, sprich ca. 72 Billiarden möglichen Schlüsselkombinationen) geknackt werden.

1996

https://

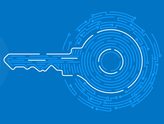
SSL

Netscape führt SSL (Secure Socket Layer) Version 3 ein, bei der die Identität der Server mithilfe elektronischer Zertifikate überprüft wird, die im Netscape-Browser Navigator integriert sind.

1999

TLS

SSL Version 3.0 wird von Transport Layer Security (TLS 1.0) abgelöst.



2005

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

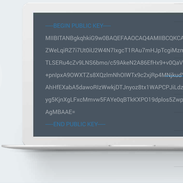
ECC

Die amerikanische Sicherheitsbehörde NSA (National Security Agency) empfiehlt die elliptische Kurven-Kryptographie (ECC) für die Erzeugung von Signaturen und den Austausch von Schlüsseln.

2014

2048 BIT

NIST-Stichtag für die Umstellung von SSL-Zertifikaten mit 1024-Bit- auf 2048-Bit-Schlüssel:



2048 BIT

Bericht der National Academy verweist auf die Einschätzung von DigiCert, dass das Knacken eines 2048-Bit-RSA-Schlüssels mit herkömmlicher Computertechnologie mehrere Billiarden Jahre dauern würde.

2029

QUANTENCOMPUTER

Das NIST vermutet, dass 2048-Bit-Schlüssel noch im nächsten Jahrzehnt mit Quantencomputern innerhalb weniger Monate geknackt werden können und läutet damit offiziell das Zeitalter der Quantenkryptografie ein.

digicert®

DIGICERT MACHT DEN QUANTENSPRUNG

Es ist nur noch eine Frage der Zeit, bis Quantencomputer die Verschlüsselungsstandards RSA und ECC hinfällig machen. Bleiben Sie dem Wandel voraus und informieren Sie sich in unserem PQC-Toolkit (Post-Quantum Cryptography).

DigiCert.com/PostQuantum