digicert®

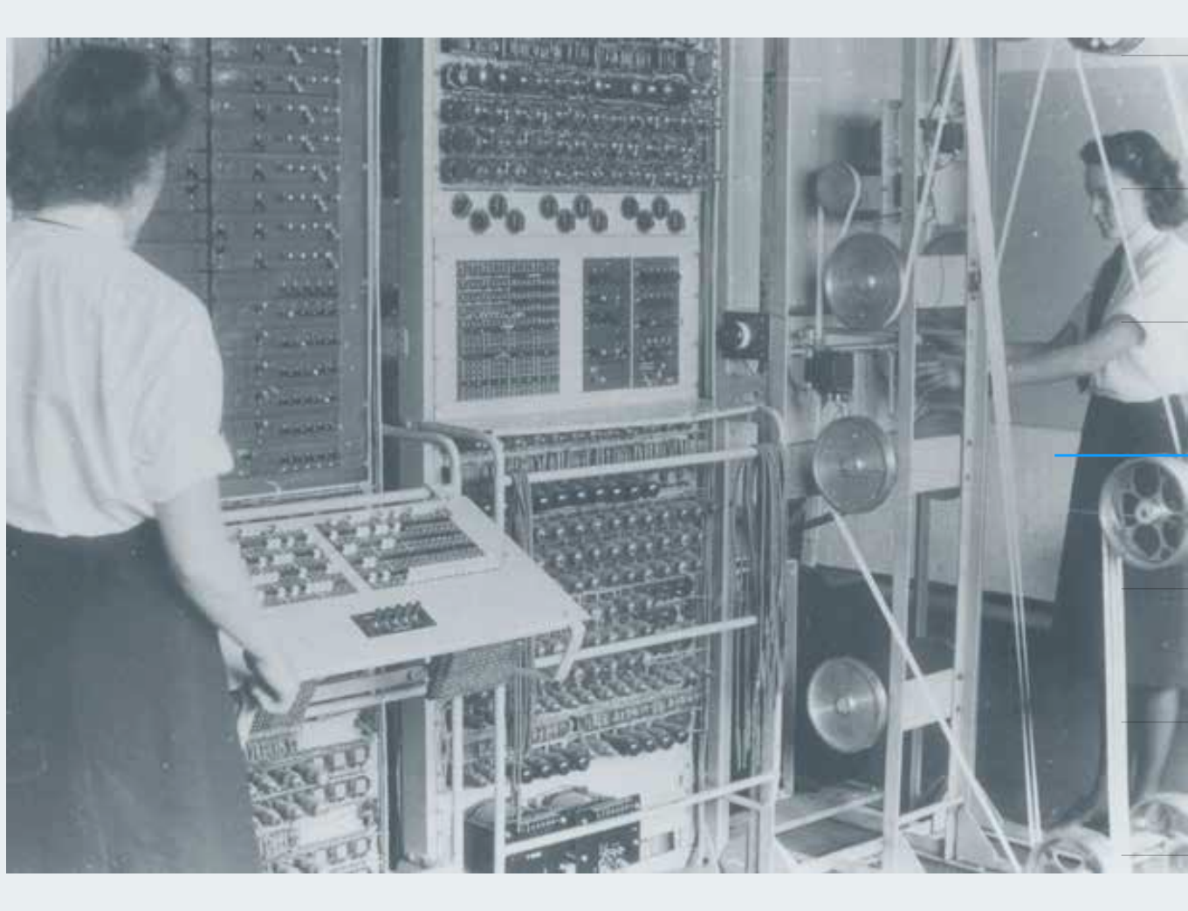
LA CRIPTOGRAFÍA
EN LA ERA DE LA COMPUTACIÓN

La historia de la criptografía es un ciclo en el que la creación de un nuevo algoritmo criptográfico va seguida de la invención de un nuevo método de descifrado. La siguiente fase del ciclo es la criptografía cuántica, que utiliza el ángulo de oscilación de un fotón para recibir los datos cifrados.

1974

BLETCHLEY PARK

Se revela la información sobre la implicación de Bletchley Park en el descifrado del código Enigma, con lo que pasa a ser de dominio público el papel de la computación a la hora de descifrar códigos.



1976

NIST

El NBS (más tarde, NIST) aprueba el estándar de cifrado de datos (DES), que posteriormente se convierte en el cifrado estándar en el mundo.

RSA®

El cifrado RSA es el primer sistema de criptografía de clave pública que utiliza una clave pública accesible a todo el mundo para cifrar los datos y una clave privada que solo conoce el destinatario para descifrarlos.

1994

CLAVE DES

Gracias a los avances en la potencia de procesamiento, ahora es posible descifrar la clave DES (con unos 72 cuatrillones de combinaciones, o 2 elevado a la 56.ª potencia).

1996

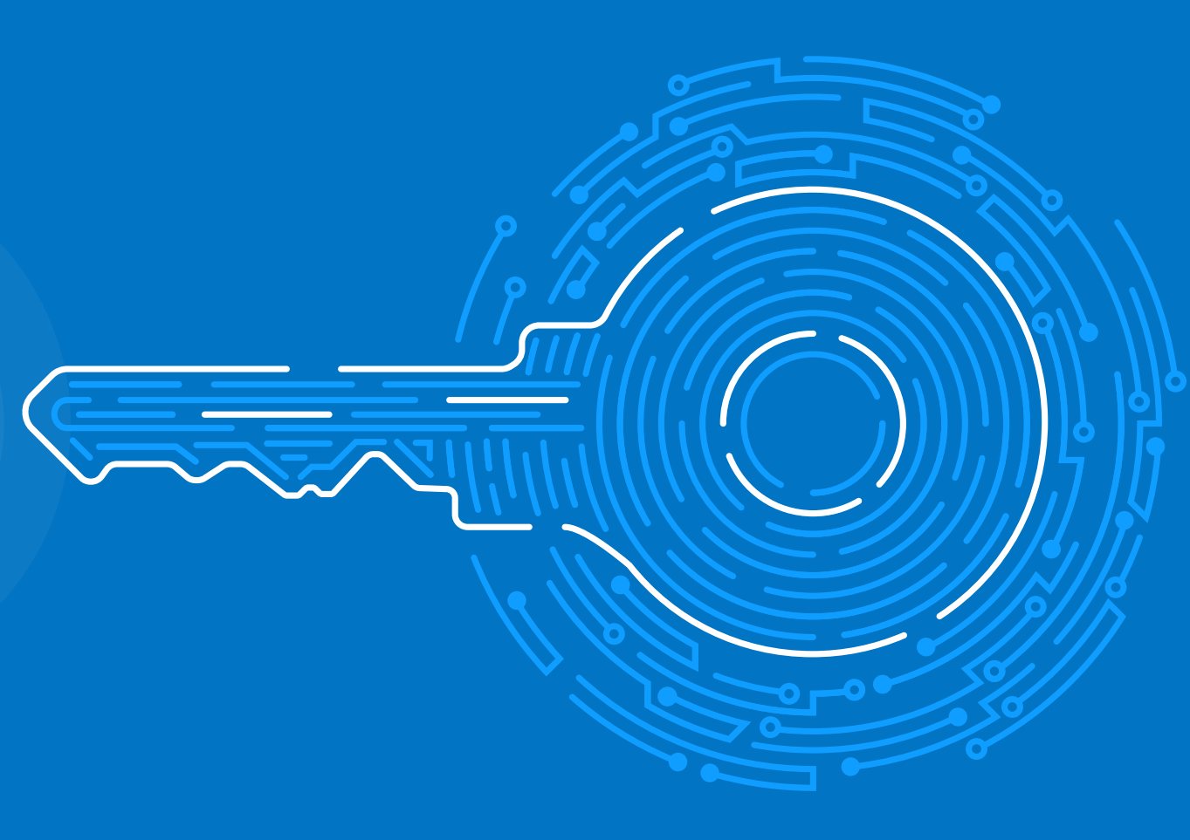
SSL

Netscape lanza la versión 3 de Secure Sockets Layer (SSL), que utiliza certificados electrónicos que comprueban explícitamente la identidad del servidor, y la inserta en su navegador Navigator.

1999

TLS

Llega el protocolo Transport Layer Security (TLS) 1.0, que se definió como una mejorade la versión 3.0 de SSL.



2005

ECC

La Agencia de Seguridad Nacional de EE. UU. presenta Suite B, que utiliza exclusivamente la criptografía de curva elíptica (ECC) para generar firmas digitales e intercambiar claves.

2014

2048 BITS

Plazo del NIST para pasar de los certificados de 1024 bits a los de 2048 bits.

```
-----BEGIN PUBLIC KEY-----
MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCA
ZWeLqiRZ7i7Ut0iU2W4N7IxgcT1RAu7mHJpTcgiMzm
TLSERu4cZv9LNS6bmo/c59AkeN2A86EfHx9+v0QaV
+pnIpxA9OWXTZs8XQzlmNhOIWTx9c2xjRp4MNjkudY
AhHfEXabA5dawoRIzWwkjDTJnyoz8tx1WAPCPJiLdz
yg5KjnXgLFxcMmvw5FAYe0qBTkKXPO19dplos5Zwp
AgMBAAE=
-----END PUBLIC KEY-----
```

2019

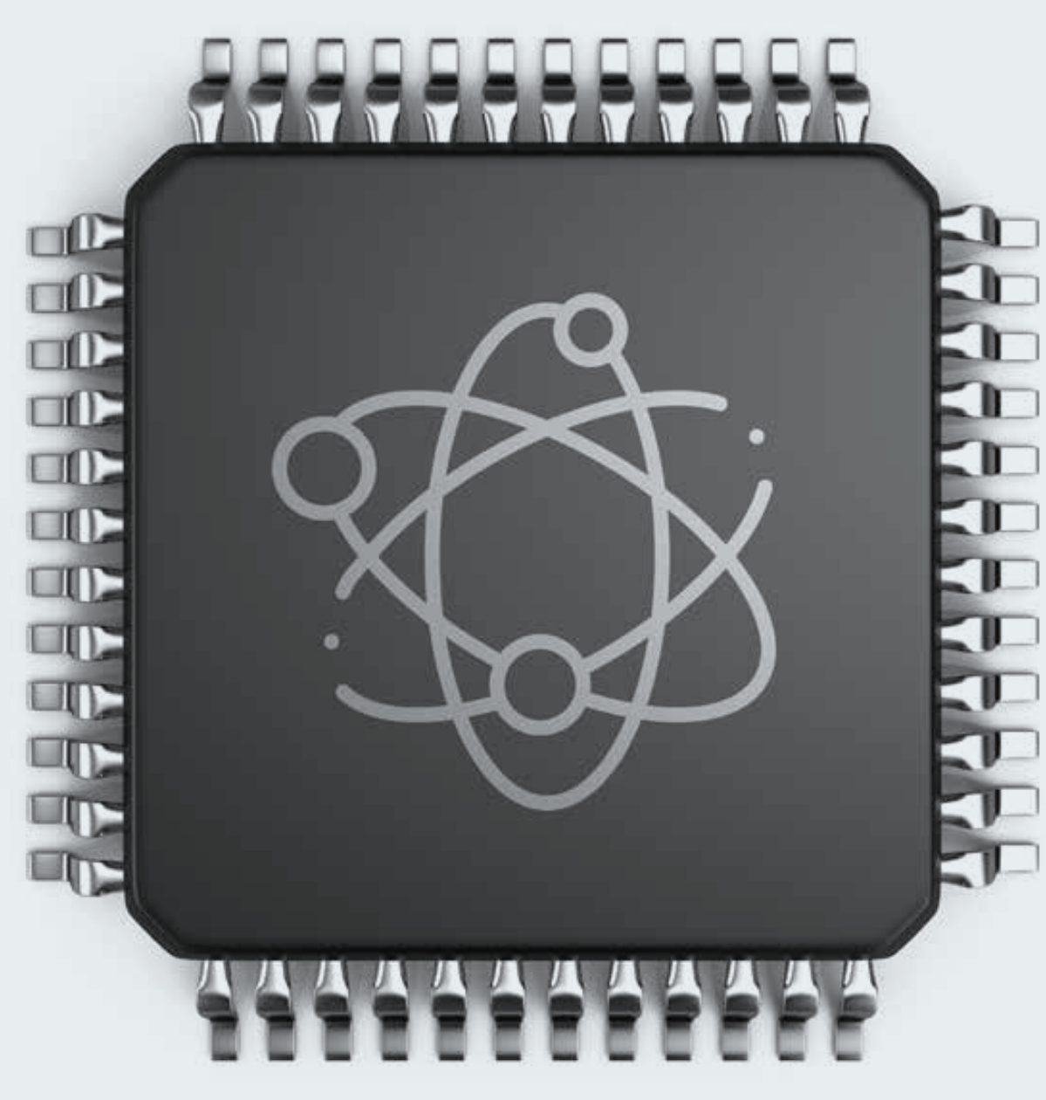
digicert®

En un informe de la National Academy se hace referencia al cálculo de DigiCert, según el cual con la computación clásica se tardaría cuatrillones de años en descifrar una clave RSA de 2048 bits.

2029

QUANTUM

El NIST calcula que la próxima década, la computación cuántica podrá descifrar esa misma clave de 2048 bits en cuestión de meses, con lo que da paso oficialmente a la era de la criptografía cuántica.



digicert®

EL SALTO CUÁNTICO

La computación cuántica pondrá patas arriba los estándares de cifrado RSA y de criptografía de curva elíptica (ECC). No sabemos exactamente cuándo, pero sin duda ocurrirá. Para ir un paso por delante, eche un vistazo a nuestro kit de herramientas de criptografía postcuántica (PQC).

DigiCert.com/PostQuantum