Intercambio de claves de Diffie y Hellman

Adrián Racero Serrano
Juan Manuel Cardeñosa Borrego

Tabla de contenidos

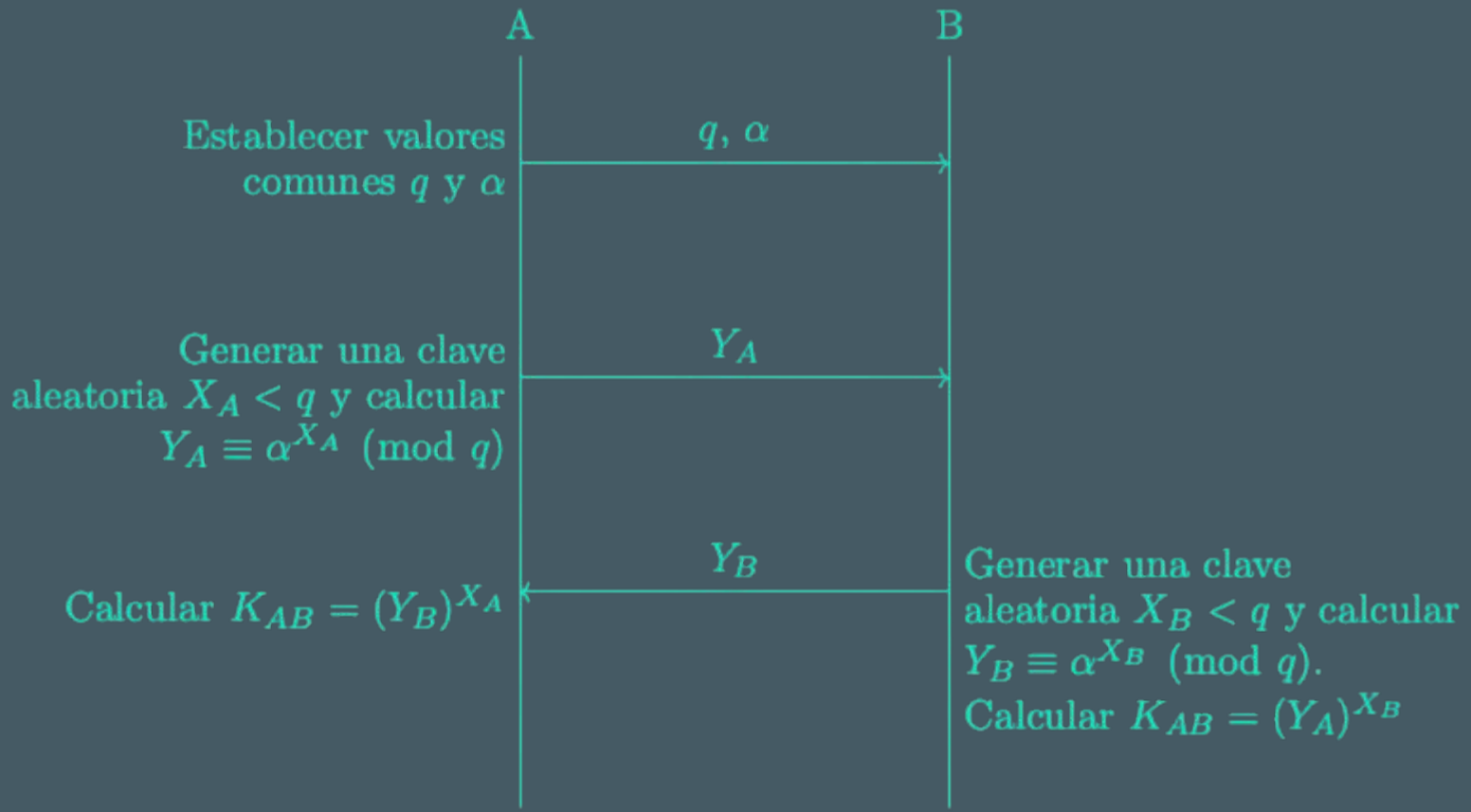
01
Introducción

- Creación en 1976.
- Intercambio de claves.
- Premio A.M. Turing 2015.
- Vulnerabilidades.

Whitfield Diffie

Martin Hellman

02
Algoritmo


A
B
Establecer valores comunes q y α
q, α
Generar una clave aleatoria $X_A < q$ y calcular $Y_A \equiv \alpha^{X_A} \pmod{q}$
Y_A
Y_B
Calcular $K_{AB} = (Y_B)^{X_A}$
Generar una clave aleatoria $X_B < q$ y calcular $Y_B \equiv \alpha^{X_B} \pmod{q}$.
Calcular $K_{AB} = (Y_A)^{X_B}$

03
Difusión y confusión

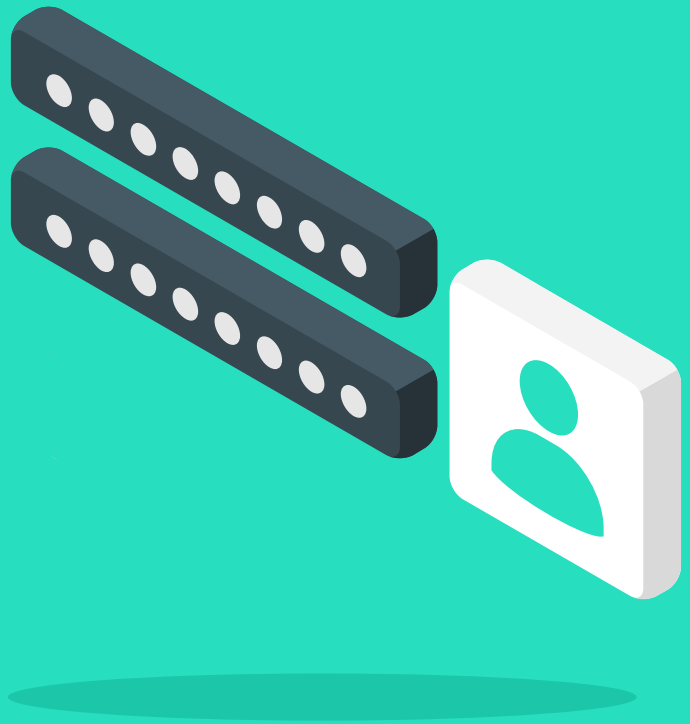
Confusión

Relación entre el texto cifrado y la clave compleja y difícil de entender.

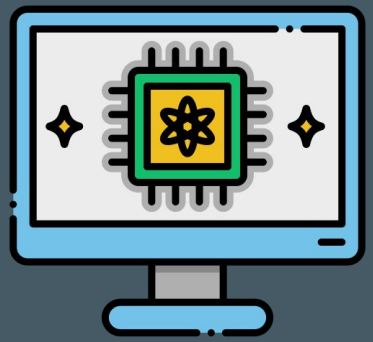
Difusión

Cada carácter del texto cifrado ha de depender de diferentes partes de la clave.

04
Vulnerabilidades



Autenticación



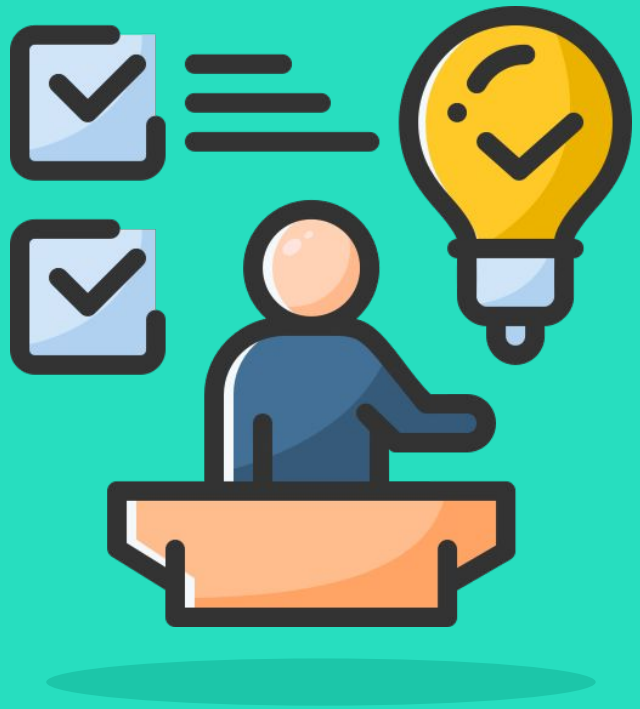
Computación cuántica

Tipos de Diffie-Hellman

- DH anónimo.
- DH estático.
- DH efímero.

RSA

05
Conclusión



¡Gracias!

Repositorio del trabajo: