CRIPTOGRAFÍA CUÁNTICA PARA DUMMIES: CÓMO ALICE Y BOB CREAN UNA CLAVE SECRETA CON FOTONES 🧬🔐

🧩¿Qué es BB84?

Es un protocolo de criptografía cuántica que permite a dos personas (Alice y Bob) crear una clave secreta segura incluso si alguien espía (como Eve).

🔍¿Qué hace Bob?

Bob no sabe la base que usó Alice, así que también elige una al azar.
Luego mide el fotón. Si su base coincide con la de Alice, el bit es correcto.
Si no, obtiene un valor al azar.
🧪 Resultado: A veces Bob acierta, a veces no.

👾 ¿Y si Eve espía?

Si Eve intercepta los fotones, tiene que elegir bases al azar.
❌ Esto introduce errores detectables cuando Alice y Bob comparan una parte de los bits.
🔍 Si hay errores: ¡Hay espía!
✅ Si no: ¡Clave segura!

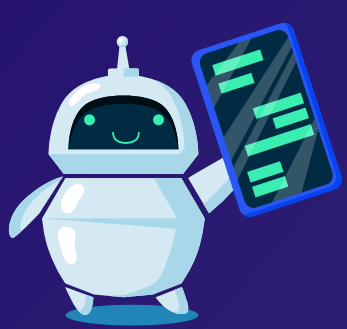
🎲El azar como protección

Alice envía bits usando fotones polarizados de forma aleatoria:

- ↕ Representa una base recta (| y —)
- ↗ Representa una base diagonal (/ y \)

Ella lanza dos monedas:

- Una elige el bit (0 o 1)
- Otra elige la base (↕ o ↗)



🔐 Clave secreta compartida

Alice y Bob comparan las bases por un canal público (no los bits).
✅ Se quedan solo con los bits donde las bases coinciden.
✨ ¡Esa es la clave secreta cuántica!

🎯 BB84 explicado con un ejemplo simple

👩 1. Alice quiere enviar 8 bits
Ella elige 8 bits al azar:
Bits de Alice: 1 0 1 1 0 0 1 0

🎲 2. Alice elige bases al azar (↕ o ↗)
Por cada bit, lanza una moneda para elegir la base:
Bases de Alice: ↕ ↗ ↗ ↕ ↕ ↗ ↗ ↕

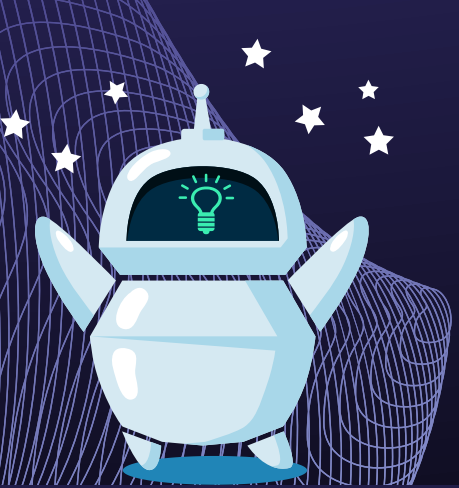
🔦 3. Alice envía los fotones polarizados
Cada fotón lleva su bit con la base correspondiente.

👱 4. Bob también elige bases al azar
Bob no sabe qué base usó Alice, así que también lanza su moneda:
Bases de Bob: ↗ ↗ ↕ ↕ ↕ ↕ ↗ ↕

🧪 5. Bob mide los fotones
Si su base coincide con la de Alice, obtiene el bit correcto. Si no, es un valor al azar. Supón que mide:
Bits de Bob: ? 0 ? 1 0 ? 1 0

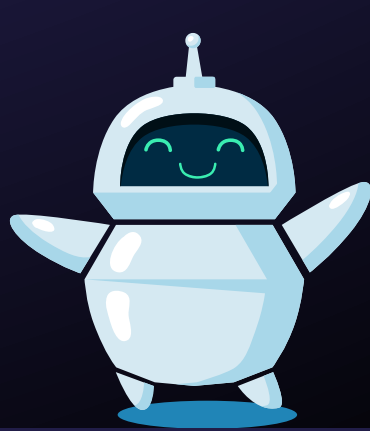
📡 6. Comparan bases públicamente
No revelan los bits, solo las bases:
Coincidencias: ✗ ✓ ✗ ✓ ✓ ✗ ✓ ✓

🔐 7. Forman la clave con los bits coincidentes
Solo guardan los bits donde las bases coincidieron:
Clave secreta: 0 1 0 1 0
✅ ¡Ahora Alice y Bob tienen una clave secreta compartida!



🚀¿POR QUÉ IMPORTA?

- La criptografía cuántica no puede ser rota ni por supercomputadoras cuánticas.
- 🔮 ¡Es el futuro de la seguridad digital!



Fabian Juarez 21440
Jennifer Toxcon 21276