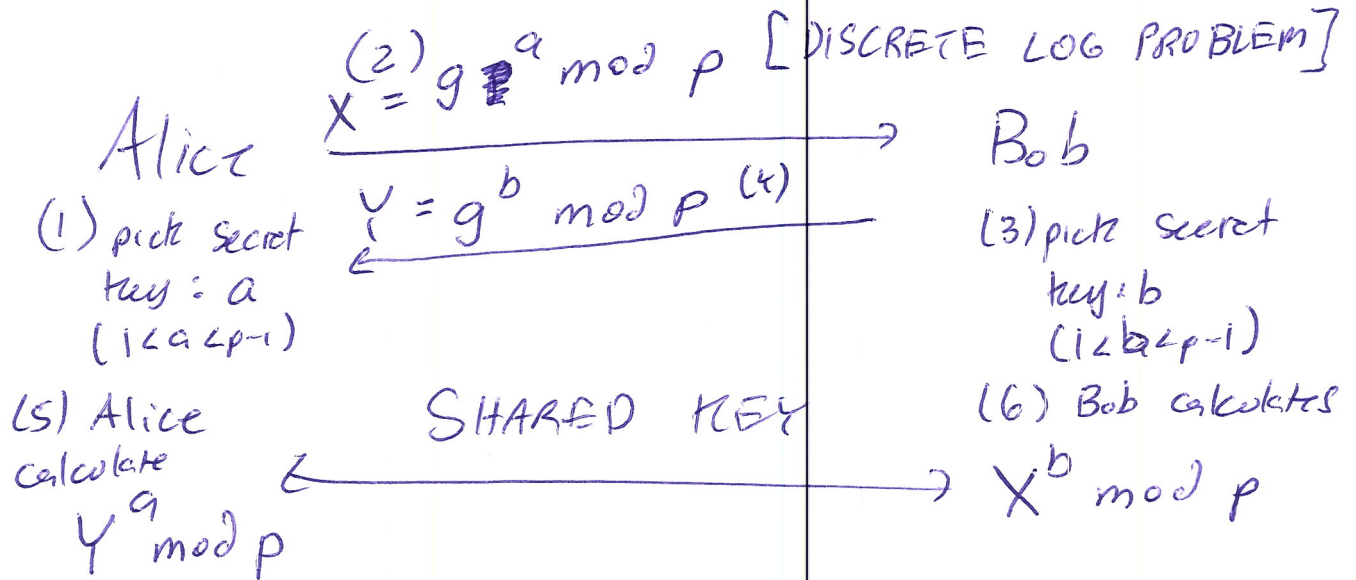


Diffie-Hellman Key Exchange

Alice → Pick a large prime number (p)
Bob → Pick a generator/primitive root mod p (g)
→ PUBLIC ELEMENTS



$$Y^a = (g^b)^a \equiv g^{ab} \pmod p$$

$$X^b = (g^a)^b \equiv g^{ab} \pmod p$$

$$XY = (g^a)(g^b) \equiv g^{a+b} \pmod p$$

↓ ↓
interceptor

DOES NOT HELP

Small Examples

$$p = 13$$

$$g = 2$$

Alice picks
 $a = 5$

$$2^{85} = 32 \equiv 6 \pmod{13}$$

Bob picks
 $b = 9$

$$2^9 = 512 \equiv 5 \pmod{13}$$

$$5^5 \pmod{13}$$

$$6^9 \pmod{13}$$

1	2	3	4	5
5	-1	-5	1	5

1	2	3	4	5	6	7	8	9
6	10	8	9	2	-1	-6	3	5

$$(2^9)^5$$

SAME

$$(2^5)^9$$

RSA Encryption

Rivest
Shamir
Adleman



Story from Code Book

Alice (Set up public keys so she can send her a message)

Bob

1. Pick 2 large primes p, q (Private keys)
2. Calculate $n = p \cdot q$ (Public key)
3. Calculate $\phi(n) = (p-1)(q-1)$ [can't be shared!]
4. Choose a random value e , such that $\gcd(e, \phi(n)) = 1$. [Public key]
5. Calculate $d \equiv e^{-1} \pmod{\phi(n)}$ [Private key]

Public Keys

n, e

Private Keys

p, q, d , ($\phi(n)$ must be kept private)

Bob to send message to Alice:

$0 < m < n$ Calculates $C = M^e \pmod n$

Alice receives C , Calculates $C^d \equiv M \pmod n$

$$C^d \equiv (me)^d \equiv M^{ed} \equiv M^{k\phi(n)+1}$$

Since $d \equiv e^{-1} \pmod{\phi(n)}$, $de \equiv 1 \pmod{\phi(n)}$,
There exists some int. k s.t. $de = k\phi(n) + 1$.

$$\equiv M^{k\phi(n)} \cdot M^1$$

$$\equiv (M^{\phi(n)})^k \cdot M^1$$

$$\equiv (1)^k \cdot M^1, \text{ provided } \gcd(M, n) = 1$$

$$\equiv M \pmod{n}$$