CIS3362 10/27/21

Diffie-Hellman Key Exchange

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

(2) $X = g^a \bmod p$ [DISCRETE LOG PROBLEM]

Alice → Bob

Bob → Alice: (4) $Y = g^b \bmod p$

(1) Alice picks secret key: a ($1 < a < p-1$)

(3) Bob picks secret key: b ($1 < b < p-1$)

(5) Alice calculates $Y^a \bmod p$

SHARED KEY

(6) Bob calculates $X^b \bmod p$

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

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

$$XY = (g^a)(g^b) \equiv g^{a+b} \bmod p$$] DOES NOT HELP

XY ↓ intercepted

Small Examples

$p = 13$ $g = 2$

Alice picks $a = 5$

$2^5 = 32 \equiv 6 \pmod{13}$ →

Bob picks $b = 9$

← $2^9 = 512 \equiv 5 \pmod{13}$

$5^5 \bmod 13$

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

$6^9 \bmod 13$

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 any can send her a message)

Bob

1. Pick 2 large primes = p, q (Private keys)
2. Calculate $n = p \cdot q$ (Public key)
3. Calculates $\phi(n) = (p-1)(q-1)$ [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 $C = M^e \bmod n$

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

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

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

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

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

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

$$\equiv M \bmod n$$