CIS 3362 11/2/26

1. finish up Diffie-Hellman
2. RSA
3. El Gamal

Diffie Hellman

Alice picks prime p, generator g (Public Elements)

Alice pick private key a $\xrightarrow{g^a \bmod p}$ Bob

$\xleftarrow{g^b \bmod p}$

to Alice

$\downarrow$

$(g^b)^a \bmod p$

So Alice + Bob never reveal their private keys

Bob pick private key b

$\downarrow$

$(g^a)^b \bmod p$

Eve can't figure out a or b due to difficulty of the Discrete Log Problem.

RSA - Rivest, Shamir, Adelman

Similar to Diffie-Hellman, they sought a public key cryptosystem.

Rivest, Shamir → COME UP W/ IDEAS

Adamen → SHOOT IDEAS DOWN!

1975 - 1977 era (very close to Diffie-Hellman timeline)

↳ Christmastime 1976

Rivest at party, has eureka moment

- gets home
- puts together entire paper working all night

full week Adelman couldn't find flaws

⟹ Decided to publish it early 1977

RSA - lets anyone send a message to Alice and only Alice can read it!

Alice picks Private elements $p, q \in$ Prime (large)

Alice computes public key $n = pq$.

Alice computes $\phi(n) = (p-1)(q-1)$

Alice picks e, $\gcd(e, \phi(n)) = 1$

Public key are $\boxed{n, e}$.

Alice compute $d = e^{-1} \bmod \phi(n)$.

Alice's Private key is $\boxed{d}$.

If Bob wants to send message, M, to Alice $0 < m < n$, he computes $C = M^e \bmod n$ sends to Alice.

Alice receives C, computes $M' = C^d \bmod n$, recovering the message (so $M' = M$ should be equal)

$$M' = C^d = (M^e)^d \bmod n$$

$ed \equiv 1 \bmod \phi(n)$ by def mod

$ed = k\phi(n) + 1, k \in \mathbb{Z}$.

$$= M^{ed} \bmod n$$

$$= M^{k\phi(n)+1} \bmod n$$

$$= M^{k\phi(n)} \times M \bmod n \equiv (M^{\phi(n)})^k \times M \bmod n$$

$$\equiv 1^k \times M \equiv M \bmod n$$

We'll assure $\gcd(M, n) = 1$. If not don't send. Would be rare where n.

Exercise: Given n, $\phi(n)$ for RSA keys find p, q.

SIDEBAR

British Security Agency was also working on developing public key cryptography in the 1970s.

Clifford Cocks - IMO (International Math Olympiad) participant

graduates college gets job w/ govt in security.

~ 22-24 yrs old.

established researchers tell Clifford about the public key problem...

In the span of 3 weeks in 1972, Clifford came up with BOTH RSA + Diffie-Hellman on his own.

Clifford's NDA only expired in 1997. (~25yrs)

RSA2 Code

$$BRICK = 1\times26^4 + 17\times26^3 + 8\times26^2 + 2\times26^1 + 10\times26^0$$

O

$26\times0 + \overset{B}{1} = 1$

$26\times1 + \overset{R}{17} = 43$

$26\times43 + \overset{I}{8} = \underbrace{1\times26^2 + 17\times26 + 8}_{C}$

$26(1\times26^2 + 17\times26 + 8) + 2 =$

$26\left(1\times26^3 + 17\times26^2 + 8\times26^1 + 2\right)$.

$26\left(1\times26^3 + 17\times26^2 + 8\times26^1 + 2\right) + 10$ K

El Gamal

Anyone can send a message to Alice.

Public elements: $q \in$ Prime

α is a generator mod q.

Alice's Private key $= X_A$, $1 < X_A < q$.

Alice's Public key $= Y_A = \alpha^{X_A} \bmod q$.

How Bob sends a message

1. Msg is M, $1 < M < q$.
2. Bob picks random value, k, $1 < k < q-1$.
   Note: each different choice of k results in a different ciphertext.
3. Bob computes $K = Y_A^k \bmod q$. (like 2nd part of Diffie-Hellman)
4. Bob sends to Alice Ordered Pair (C_1, C_2)

$$C_1 = \alpha^k \bmod q$$ (what Bob would send to Alice in Diffie-Hellman)

$$C_2 = K \cdot M \bmod q$$

Note $K^{-1} \times C_2 \equiv (k^{-1})(k)(M) \bmod q$
$\equiv 1 \times M \equiv M \bmod q$

Alice needs to compute K^{-1}

1. Alice compute $C_1^{x_A} = (\alpha^k)^{x_A} = K$

Note $K = (Y_A)^k = (\alpha^{x_A})^k = \alpha^{x_A k}$

2. Alice runs mod Inverse to compute $K^{-1} \bmod q$

3. Alice multiplies result from step 2 times C_2 to get plaintext.