CIS 3362 10/29/25

1) Addendum to RSA/Diffie-Hellman Story
2) RSA code
3) H6
4) Start El Gamal (next Public Key Cryptosystem)

Clifford Cocks joins British Security Agency
↳ works w/ Martin Williamson. Friends from before participated 1968? International Math Olympiad (IMO)

Comes up with RSA back in 1973 in a few days ("took like 30 minutes max").
Bad News: He + Brit Gov couldn't tell anyone!
In 1974 or 5 he also discovered Diffie-Hellman
Declassified in 1997

$$UCF = 20 \times 26^2 + 2 \times 26^1 + 5 \times 26^0$$

20 2 5

$$UC = (20 \times 26^1 + 2 \times 26^0)$$

val ↙ val + num (new #)

$$UCF = 26(20 \times 26^1 + 2 \times 26^0) + 5 \times 26^0$$

$$20 \times 26^2 + 2 \times 26^1 + 5 \times 26^0$$

El Gamal

- Slower than RSA
- A bit more complicated } not used as much as RSA

Alice will create her own private/public keys

1. Alice chooses public elements, q (large prime) and α (generator of q). mod
2. Alice computes $Y_A = \alpha^{X_A}$, where $1 < X_A < q$, and is Alice's secret key. Y_A is public key.

public elements → q, α, Y_A ← her public key

Alice posts: q, α, Y_A

Bob wants to send message to Alice

1. Let plaintext $= M$ $\quad 0 \leq M \leq q-1$.
2. Bob chooses a random int k, $1 \leq k \leq q-1$, and selects a different one for each block.
3. Bob calculates $K = Y_A^k \bmod q$.
4. Bob sends following to Alice

$C_1 = \alpha^k \bmod q$ (k ← lowercase) $\quad C_2 = K \cdot M \bmod q$ (K ↑ CAPITAL)

How Alice recovers M

1. Alice computes $K = C_1^{X_A} \bmod q$

Proof: $C_1^{X_A} = (\alpha^k)^{X_A} = (\alpha^{X_A})^k = Y_A^k = K$ ✓

2. Alice uses EEA to calculate $K^{-1} \bmod q$.

3. Alice computes $K^{-1} \times C_2 = M$.

$K^{-1}(K \cdot M) = (K^{-1} \cdot K) \cdot M \equiv 1 \cdot M \bmod q$