CS 70 ## 2.18 LECTURE 9

GOAL

To allow anyone to encrypt w/public knowledge.
But only we can decrypt w/secret knowledge.

IDEA

We know p & q, everyone knows $N = pq$
Try x^e mod N. Works, but not secret.
Try xe mod N. Works if e coprime to N, but not secret.
Try x^e mod N. Call this y.

Invert: $y_p = y \bmod p$ ↳ $= x_p^e \bmod p$ $\quad y_q = y \bmod q$ ↳ $= x_q^e \bmod q$ where $x_p = x \bmod p$, $x_q = x \bmod q$

We know exponentiation is cyclic w/period $p-1$.
If e is coprime to $p-1$ & $q-1$, FLT applies.
Compute e_{p-1}^{-1} & e_{q-1}^{-1} (multiplicative inv. mod $p-1$, $q-1$)
Compute $y_p^{e_{p-1}^{-1}}$ & $y_q^{e_{q-1}^{-1}}$ mod respective $= x_p$ & x_q

EX $p=5$ $q=11$ → $N=55$ ①
$p-1=4$ $q-1=10$ → $e=3$
$e_4^{-1} = 3$ | $e_{10}^{-1} = 7$ → $x=13 \to \begin{bmatrix} 13 \bmod 5 \\ 13 \bmod 11 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$ ⑤ next line
→ $y = 13^3 \bmod 55 = 52 \to \begin{bmatrix} 2 \\ 8 \end{bmatrix}$ ③
Invert: $2^3 = 8 \bmod 5 = 3$ ④
$8^7 \bmod 11$ (repeated squaring)
$8^1 \equiv 8$ $8^2 \equiv 9$ $8^4 \equiv 4$
$8^7 = 2 \bmod 11 = 2$ ⑤ start of line
→ $\begin{bmatrix} 3 \\ 2 \end{bmatrix} \to 3v_5 + 2v_{11} \bmod 55 = 123$ ⑥
↳ $5 \mid 11$ ↳ $4 \mid 5$ → $= 13$ ✓

SECRET SHARING

Any k people can come together and recover the secret, but fewer than k get nothing at all. For example we want any 432 people of 10000 to be able to decode.