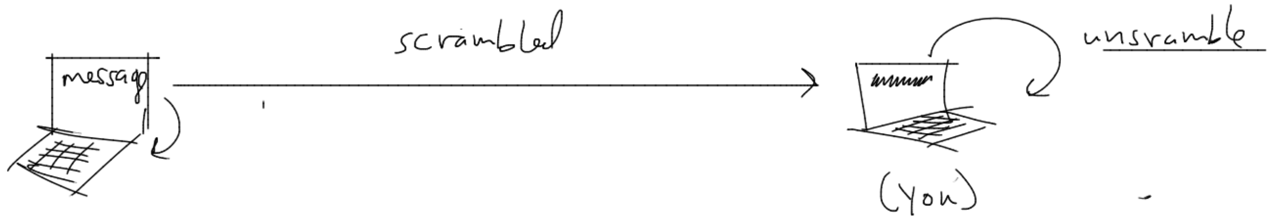
Monday – Week 11

Projects: History Topic?
• make it unique.

Today: RSA encryption
(application of group theory to online security)

• 2002: Won "Noble Prize of computing"

• RSA is everywhere



public-key cryptography.

You make public a key (large #) n & a scrambler (integer) k. exponent

Anyone can send a "secret" message to you by:

1. Their message $M =$ "HEY" first is coded as:

$$\begin{array}{cccccc} A & B & \ldots & Z & \sqcup \\ | & | & & | & | \\ 1 & 2 & & 26 & 27 \end{array} \quad \text{so } M = \underbrace{08\ 05}_{M_1}\ \underbrace{25}_{M_2}$$

$$M = 0805 \quad 2527$$

2. Encrypt: $0805^k \bmod n = 0805^{11} \bmod 899 = 557$ → what is sent across web.

$(n = 29 \cdot 31)$

assume $k = 11$

3. Decryption: $\boxed{d}$ Finding this exponent is "impossible" given just n & k.

$$557^{d} \bmod n = 0805$$

d is known to be the "inverse of k"

so that $\quad 1 \text{ in group}$

$$\text{HEY} = (0805)^k = (557)^d = 0805^{kd} = 0805$$

RSA starts w/ 2 "large primes" — known by receiver.

For us: $p = 29$, $q = 31$. product $n = 29 \cdot 31 = 899$

The first exponent (scrambler) this only needs to rel. prime to $m = \text{lcm}(p-1, q-1)$ $\quad m = (p-1)s$

$m = \text{lcm}(\underset{2 \cdot 2 \cdot 7}{28}, \underset{5 \cdot 2 \cdot 3}{30}) = 420$ $\quad m = (q-1)t$

Choose $e = 11$.

message M = WILD = 23 9 12 4 = [2309] [1204]
$= M_1 \; M_2$

$M_1^e = 2309^{11} \bmod 899 = 77$
$M_2^e = 1204^{11} \bmod 899 = 688$
encrypted messages

$U(5) = \{1, 2, 3, 4\}$

$M_1 = 2309$ is relatively prime to $n = 899$
rel. prime

so $M_1 \in U(899) = U(29 \cdot 31) = U(29) \oplus U(31) = \mathbb{Z}_{28} \oplus \mathbb{Z}_{30}$

$M_2 \in U(899) = U(29 \cdot 31) = U(29) \oplus U(31) = \mathbb{Z}_{28} \oplus \mathbb{Z}_{30}$

also recall e is rel. prime to $m = \text{lcm}(29-1, 31-1)$
$= 420$

choose decrypting exponent d s.t.

$ed = 1 \bmod m = 1 \bmod 420$

$\boxed{ed = 1 + mq} = ed = 1 + 420q$

$11 \cdot d = 1 + 420q$

$\Rightarrow \boxed{d = 191}$

Take any message $x \in U(899)$

$x^m = (\underset{\mathbb{Z}_{28}}{x_1}, \underset{\mathbb{Z}_{30}}{y_1})^m = (x_1^m, y_1^m) = \left((x_1^{28})^s, (x_2^{30})^t\right) = (0, 0) = 1 \in U(899)$

$m = 28s$
$= 30t$

$\Rightarrow$ m kills any message

$M_1^e \longrightarrow (M_1^e)^d = M_1^{ed} = M_1^{1+mq} = M_1 \cdot M_1^{mq} = M_1 (M_1^m)^q$
$= M_1 \cdot 1 = M_1$