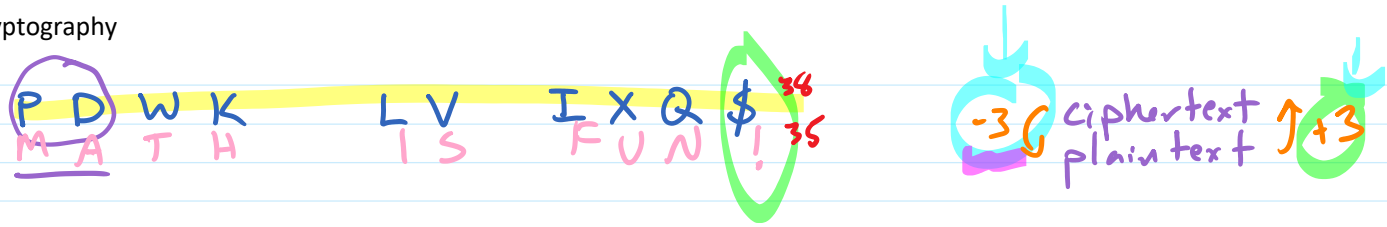
Cryptography



encryption key: used to transform plaintext → ciphertext

decryption key: used to transform ciphertext → plaintext

Goal: allow anyone to send you an encrypted msg w/o prior key exchange

difficult for anyone other than recipient to decrypt message

public key: encryption key — not secret - post anywhere

private key: decryption key — secret; will be related to encryption key but must be related in a way that makes it difficult to recover private from public

THM (Fermat's Little Theorem): For any prime p and $a \in \mathbb{Z}$ not a multiple of p,

then $a^{p-1} \equiv 1 \pmod p$

and $a^p \equiv a \pmod p$

$143 = 11 \cdot 13$ (p, q)

$143 \% 2 = 1$, $143 \% 3 = 2$, $143 \% 5 = 3$, $143 \% 7 = 3$, $143 \% 11 = 0$

$p = 7$

n	1	2	3	4	5	6
$n^6 \bmod 7$	1	$64 \equiv_7 1$	$3^6 = (3^2)^3 \equiv_7 2^3 \equiv_7 1$	$(4^2)^3 \equiv_7 2^3 \equiv_7 1$	$(5^2)^3 \equiv_7 4^3 \equiv_7 1$	$(6^2)^3 \equiv_7 1^3 \equiv_7 1$

common sizes of n: hundreds of digits

$\operatorname{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}$ $\quad \operatorname{lcm}(4,6) = 12$

RSA

public key: $n = p \cdot q$ for primes p, q

$e \in \mathbb{Z}$ s.t. $\gcd(e, \operatorname{lcm}(p-1, q-1)) = 1$

private key: $d \in \mathbb{Z}$ s.t. $d \cdot e \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$

(and $p > q$, d_p s.t. $d \equiv d_p \pmod{p-1}$ $\quad 0 \le d_p < p-1$

d_q s.t. $d \equiv d_q \pmod{q-1}$ $\quad 0 \le d_q < q-1$)

ciphertext

To encrypt: find c s.t. $m^e \equiv c \pmod n$

To decrypt: find m s.t. $c^d \equiv m \pmod n$

Example: choose $p = 37$ $\quad q = 73$ so $n = 2701$

compute $\operatorname{lcm}(36, 72) = 72$ (so a bad choice of p, q better if $\gcd(p-1, q-1)$ is small)

choose $e = 5$ note $\gcd(5, 72) = 1$

find d s.t. $de \equiv 1 \pmod{72}$ so $d = 29$ $\quad 145 = 5 \cdot 29$

$5d \equiv 1 \pmod{72}$

$m = 1304$

MD → 13 04 → $(1304)^5 = 1304 \cdot (1304)^4 \pmod{2701}$

(m D)

$\equiv 1304 \cdot (1304^2)^2$

$\equiv 1304 \cdot (1487)^2$

$\equiv 1304 \cdot 1751$

$\equiv 959$

$= c$

$29 = 16 + 8 + 4 + 1$

$x^{29} = x^{16} \cdot x^8 \cdot x^4 \cdot x$

$959^{29} = 959 \cdot (959^2)^2 \cdot ((959^2)^2)^2 \cdot (((959^2)^2)^2)^2$

$= 959 \cdot 1241^2 \cdot (1211^2)^2 \cdot ((1211^2)^2)^2 \pmod{2701}$

$\equiv 959 \cdot 1341^2 \cdot (1341^2)^2 \cdot ((1341^2)^2)^2 \pmod{2701}$

$\equiv 959 \cdot 2116 \cdot 2116^2 \cdot (2116^2)^2 \pmod{2701}$

$\equiv 959 \cdot 2116 \cdot 1899 \cdot 1899^2 \pmod{2701}$

$\equiv 959 \cdot 2116 \cdot 1899 \cdot 366 \equiv 1304 \pmod{2701}$

MD

Decrypt 2066 → using same private key

find plaintext that makes this work ↓

$2066^{29} \equiv \_\_\_\_ \pmod{2701}$

$\equiv 2066 \cdot 2066^4 \cdot 2066^8 \cdot 2066^{16} \pmod{2701}$

$\equiv 2066 \cdot 2554 \cdot 1 \cdot 1$

$\equiv \underset{O}{15}\,\underset{K}{11} \pmod{2701}$

$\gcd(n_i, n_j) = 1$ for $i \neq j$

THM (Sun-tzu's Remainder Theorem): If $n_1, \ldots, n_k$ are pairwise co-prime integers, and $r_1, \ldots, r_k \in \mathbb{Z}$ satisfy $0 \leq r_i < n_i$ then there is a unique integer r s.t.

$$0 \leq r < n_1 \cdot \ldots \cdot n_k \quad \text{and}$$

$$\begin{aligned} r &\equiv r_1 \pmod{n_1} \\ r &\equiv r_2 \pmod{n_2} \\ &\vdots \\ r &\equiv r_k \pmod{n_k} \end{aligned}$$

(and r', r'' satisfy iff $r' \equiv r'' \pmod{n_1 \cdot \ldots \cdot n_k}$)

There are $m \equiv r_p \pmod p$, $m \equiv r_q \pmod q$

if $m^{de} \equiv r_p \pmod p$ ($\to$ dir of iff) and $m^{de} \equiv r_q \pmod q$

then $m^{de} \equiv m \pmod{p \cdot q}$

$\gcd(3,5) = 1$

$\gcd(3,4) = 1$ $\quad \gcd(4,5)$

Ex: $n_1 = 3 \quad n_2 = 4 \quad n_3 = 5$

$n = 3 \cdot 4 \cdot 5 - 1$

	0	1	2	3	4	5	. . .	59
n mod 3	0							
n mod 4	0							
n mod 5	0							

THM: Suppose p, q are primes, $n = p \cdot q$, d, e are integers s.t. $\gcd(e, \operatorname{lcm}(p-1, q-1)) = 1$, $d \cdot e \equiv 1 \pmod{\lambda(n)}$ ($\lambda(n)$ over $\operatorname{lcm}(p-1, q-1)$)

$(m^e)^d = m^{de}$ Then $m^{de} \equiv m \pmod n$

Proof: Suppose p, q, n, d, e are as given

It suffices to show $m^{de} \equiv m \pmod p$ and $m^{de} \equiv m \pmod q$ (by Sun-tzu)

$m^{de} \equiv m \pmod p$: 2) $m \not\equiv 0 \pmod p$: note $p-1 \mid \operatorname{lcm}(p-1, q-1)$ ($\lambda(n)$)

so $\lambda(n) = (p-1)k$ for some $k \in \mathbb{Z}$

Two cases:

1) $m \equiv 0 \pmod p$ then $m^{de} \equiv 0^{de} \equiv 0 \equiv m \pmod p$

also $de \equiv 1 \pmod{\lambda(n)}$

so $de - 1 = \lambda(n) \cdot l$ for some $l \in \mathbb{Z}$

$de - 1 = (p-1) \cdot k \cdot l$ (h)

$de = 1 + (p-1) \cdot h$

$m^{de} \equiv m^{1 + (p-1)h} \equiv m \cdot (m^{p-1})^h$

$m^{de} = m^{1+(p-1)h} = m \cdot (m^{p-1})^h$

Fermat's Little Thm says $m^{p-1} \equiv 1 \pmod{n}$ since we are in the $m \not\equiv 0 \pmod{p}$ case

$\longrightarrow \equiv m \cdot 1^h \pmod{p}$

$\equiv m \pmod{p}$

$m^{de} \equiv m \pmod{q}$: similar