Lecture 2 PUBLIC KEY CRYPTOSYSTEMS

2.1. MODULAR ARITHMETIC

$a \equiv b \bmod n$ n divides $a-b$, e.g. $4 \equiv 10 \bmod 3$

$a+b \bmod n$, $a \times b \bmod n$ like a regular arithmetic

$Z_n = \{0, 1, 2 \ldots, n-1\}$ group under addition mod n

$Z_n = \{1, 2, 3, \ldots, n-1\}$ usually NOT a group under multiplication

problems with inverses

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Z_5

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

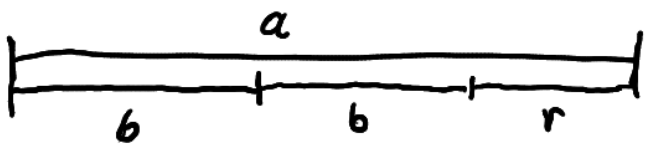
Z_6

a has reverse mod n if a is coprime with n

↓

gcd and Euclid's algorithm

2.2 EUCLID'S ALGORITHM



$\gcd(a, b) = \gcd(a-b, b)$

$\gcd(a, b) = d$

$d = xa + yb$

x, y integers (could be negative)

a, b coprime, $\gcd(a, b) = 1$

$\rightarrow xa + yb = 1$ $x \cdot a = 1 \bmod b$, $y \cdot b = 1 \bmod a$

INVERSES

$a = k_0 b + r_1$
$b = k_1 r_1 + r_2$
$r_1 = k_2 r_2 + r_3$
$r_2 = k_3 r_3 + r_4$ ← $\gcd(a, b)$
$r_3 = k_4 r_4$ ←

JUST WORK BAKWARDS

$a = 696$ $b = 13$

$696 = 53 \times 13 + 7$
$13 = 1 \times 7 + 6$
$7 = 1 \times 6 + 1$
$6 = 6 \times 1$ ← $\gcd(696, 13)$

1.3 EULER'S THEOREM

Z_n^* ← numbers co-prime with n

$Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

$\varphi(n) \rightarrow$ # of elements in Z_n^* / co-prime with n

$\varphi(p) = p-1$ if p is a prime number

$\varphi(p \cdot q) = (p-1)(q-1)$, p, q - prime

Theorem

$$a^{\varphi(n)} \equiv 1 \mod n \qquad \gcd(a, n) = 1$$

Proof

for any Abelian group $G = \{g_1, g_2, g_3, \dots g_n\}$

multiply by $g \in G$ $\{gg_1, gg_2, gg_3, \dots gg_n\}$ the same set only permuted

$$g_1 \times g_2 \times g_3 \times \dots \times g_n = (g \times g_1) \times (g \times g_2) \times (g \times g_3) \times \dots \times (g \times g_n)$$

$$= g^n \times (g_1 \times g_2 \times g_3 \times \dots g_n)$$

hence $g^n = 1$ identity

$a \in Z_n^*$ $\qquad a^{\varphi(n)} \equiv 1 \mod n$

1.4 RSA

$P^e \mod n = C$

$C^d \mod n = P^{e \cdot d} \mod n$

$= P^{k\varphi(n)+1} \mod n$

$= P^{k\varphi(n)} \mod n \cdot P \mod n$

EULER

$= 1 \cdot P \mod n$

$= P$

BOB

p, q - prime

$p \cdot q = n$

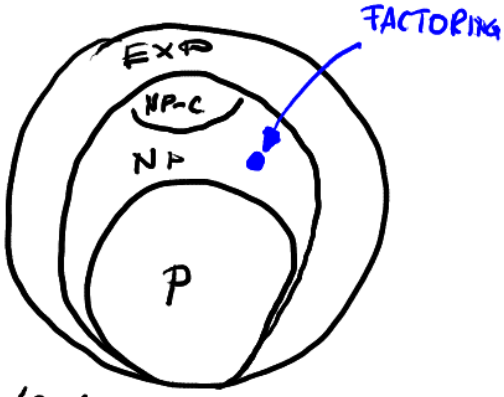
$e \cdot d = 1 \mod \varphi(n)$ — d: PRIVATE KEY

e coprime with $p-1, q-1$

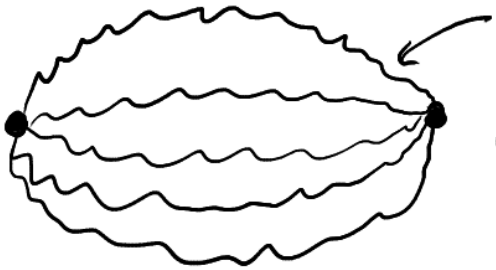
PUBLIC KEY: e, n

→ How to get d out of that?
Easy if you know $\varphi(n)$ / factors of n

1.5 IS FACTORING REALLY HARD?

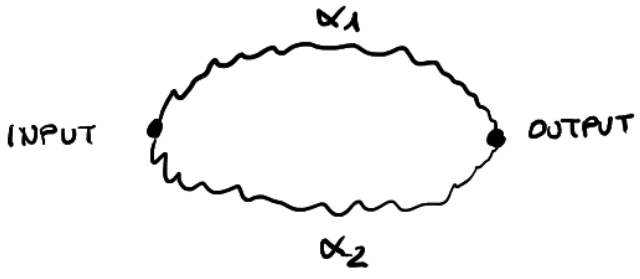


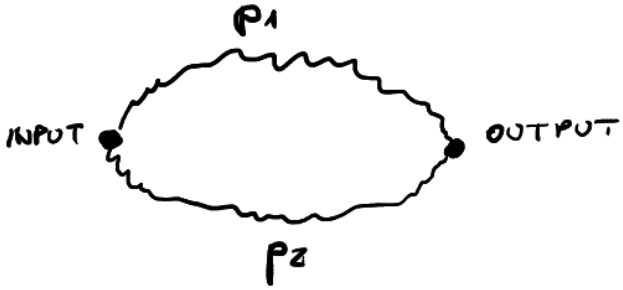
Efficient quantum algorithm



quantum computing

multiparticle quantum interference





$$p = |\alpha_1 + \alpha_2|^2 =$$

$$= |\alpha_1|^2 + |\alpha_2|^2 + \alpha_1\alpha_2^* + \alpha_1^*\alpha_2$$

$$= p_1 + p_2 + |\alpha_1| e^{i\varphi_1} |\alpha_2| e^{-i\varphi_2} + |\alpha_1| e^{-i\varphi_1} |\alpha_2| e^{i\varphi_2}$$

$$= p_1 + p_2 + 2|\alpha_1||\alpha_2| \cos(\varphi_1 - \varphi_2)$$

$$= p_1 + p_2 + 2\sqrt{p_1 p_2} \cos(\varphi_1 - \varphi_2)$$

INTERFERENCE TERM

NEGATIVE — DESTRUCTIVE

POSITIVE — CONSTRUCTIVE

INTERFERENCE

QUANTUM WORLD

$$p = p_1 + p_2$$

CLASSICAL WORLD

Depends only on the difference $\varphi_1 - \varphi_2$

spurious interaction with the environment makes φ jitter

cos averages to zero

decoherence → classical world back to adding probabilities

In quantum computation values of $f(x)$ can be represented by phase factors $\varphi(x)$ → constructive interference tells us about some global properties of $\varphi(x)$ e.g. periodicity

Given $n = p \cdot q$ $a^r \equiv 1 \bmod n$ find r. HARD

r ← QUANTUM COMPUTATION SHOR'S ALGORITHM

↓

some multiple of n

$$(a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod n$$

$p \cdot q \times k$ ☹

$k \times p \cdot q$ ☹

$k_1 p \times k_2 q$ ☺ → $\gcd(a^{r/2} \pm 1, n)$

Assumptions: r is even; $a^{r/2} \neq \pm 1 \bmod n$] Probability $\geq \frac{1}{2}$

We may need to repeat this algorithm several times

1.6 POWER OF QUANTUM COMPUTATION

Can quantum computers solve NP complete problems?

Very unlikely...