Quiz 1 Wednesday 3rd Sept (class time)

We want to test whether n is composite number.

Pick a

- If n is even or $1 < \gcd(n,a) < n$, n is composite.
- $n-1 = 2^k q$ where $2 \nmid q$
- Set $a = a^q \mod n$
- If $a \equiv 1 \pmod n$ test fails.
- Loop $i = 0, 1, \dots k-1$
  - If $a \equiv -1 \mod n$, test fails
  - Set $a = a^2$
- End i loop.

Return n is composite.

Key exchange Protocols

Diffie - Hellman key Exchange

$G = \langle g \mid g^n = 1 \rangle$ $\left(= \{ e^{2\pi i/n} \} \subset \mathbb{C}^* \right.$

private key a for Alice & private key b for Bob.
— modulo n — mod n.
so $0 \le a, b \le n-1$
A generator of the group G (cyclic) & a generator g is public.

Alice computes g^a sends to Bob
Bob " g^b sends to Alice

Alice computes $(g^b)^a = g^{ab}$

Bob computes $(g^a)^b = g^{ab}$

$K = g^{ab}$ is a common knowledge.

Apply this common knowledge.

$$\Sigma : A \longrightarrow A$$

$$m \longmapsto m + k$$

$(A = \{0, 1, 2, \ldots 25\}$

where k is "common knowledge"

Messay – Omura cryptosystem.

private key of Alice $\longrightarrow a$ (she knows a^{-1})

" " of Bob $\longrightarrow b$ (he knows b^{-1})

Message M is to be sent by Alice to B.

Alice computes M^a & Alice sends M^a to Bob

Bob computes $(M^a)^b = M^{ab}$ & he sends it to Alice.

Alice computes $(M^{ab})^{a^{-1}} = M^b$

She sends M^b to Bob.

Bob computes $(M^b)^{b^{-1}} = M$.

$A = \mathbb{Z}_n$

$a, b \in U(\mathbb{Z}_n)$ invertible elements of $\mathbb{Z}_n$.

a^{-1} & b^{-1} are in $U(\mathbb{Z}_n)$ $\quad (a^{-1} \times a = 1 \pmod{28})$

M^a or M^b or $(M^a)^b = M^{ab}$ in $\mathbb{Z}_n$

Eg., $n = p$, then $U(\mathbb{Z}_p) = \mathbb{Z}_p^{\times}$ (✗)

$\| $

$\{g^0 = 1, g, g^2, \ldots, g^{p-1}\}$

for some g. (everyone except 1 qualifies)

Eg. $n = 29$ $\quad U(\mathbb{Z}_{29}) = \{1, 2, 4, 8, 16, 3, 6, 12, 24, 19,$ (2^5, 2^9)

$9, 18, 7, 14, 28, 27, 25, 21, 13, 26, 23, 17, 5, 10, 20, 11, 22, 15\}$ (2^{15}, 2^{19}, 2^{23})

private key of Alice: 5 & Bob: 3

A → 0
B → 1
C → 2
etc.

$M = C = 2 \xrightarrow{\;\;} 2^9 = 2^5 = 3 \longrightarrow 3 \xrightarrow{\;\;} 3^3 = 8 = M^{ab}$

Alice $\qquad$ Bob.

~~2 5~~

$a = 5 = 2^{22}$

$a^{-1} = 2^{28-22} = 2^6 = 6$

$a^{-1} = 5^{-1} = 17 \pmod{28}$

$b^{-1} = 3^{-1} = 19 \pmod{28}$

$(M^{ab})^{a^{-1}} = (27)^{17}$

$= (-2)^{17}$

$= (-2) \times 2^{16}$

$= (-2) \times (2^5)^3 \times 2$

$= -4 \times 3^3$

$= -4 \times (-2) \pmod{29}$

$= 8$

M^b

$(M^b)^{b^{-1}} = 8^{19} = (8^2)^9 \times 8 = 6^9 \times 8 = (6^2)^4 \times 48$

$= 7^4 \times 19$

$= 20^2 \times 19$

$= (-9)^2 \times 19 = 81 \times 19 = (-6) \times (-10)$

$= 60 = 2 \pmod{29}$

3rd sept 12 PM ⟶ 1 PM