Chinese Remainder Theorem:

$N = p \cdot q$ $\qquad f(x) = (x \bmod p,\ x \bmod q)$.

$\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$. $\qquad \forall x \in \mathbb{Z}_N$.

$x \in \mathbb{Z}_N \quad x \mapsto (x_p, x_q) \in \mathbb{Z}_p \times \mathbb{Z}_q$.

Similarly for every element $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_q$, there exists a unique element $X \in \mathbb{Z}_N$ such that $X \mapsto (x, y)$.

For any element (x_p, x_q), how do you find its inverse.

$(x_p, x_q) = x_p \cdot (1,0) + x_q (0,1)$

If you can find some elements $1_p, 1_q \in \{0, \ldots, N-1\}$ such that $1_p \leftrightarrow (1,0)$ and $1_q \leftrightarrow (0,1)$.

p, q are relatively prime to each other.

$\therefore gcd(p,q) = 1 \Rightarrow \exists X, Y \in \mathbb{Z}$ s.t $Xp + Yq = 1$

Claim: $1_p = Y_q \bmod N$

$1_q = X_p \bmod N$.

$x \leftrightarrow (x_p, x_q)$

$x_p = x \bmod p$

$x_q = x \bmod q$.

Can we prove that

$1_p \leftrightarrow (1, 0)$ and $1_q \leftrightarrow (0, 1)$

$1_p \bmod p = (Y_q \bmod N) \bmod p$

$= Y_q \bmod p = (1 - X_p) \bmod p = 1 \bmod p$.

$1_p \bmod q = (Y_q \bmod N) \bmod q = Y_q \bmod q = 0$

Similarly, we can show that $1_q \leftrightarrow (0, 1)$.

Therefore

$(x_p, x_q) \rightarrow (x_p \cdot I_p + x_q \cdot I_q) \bmod N.$

where $I_p = Y_q \bmod N$

$\|$ $I_q = Y_p \bmod N.$

Let $N = 3 \times 5$

$Z_{15} \cong Z_3 \times Z_5.$

Find out the inverse of $(2, 4)$

If p, q are two large primes.

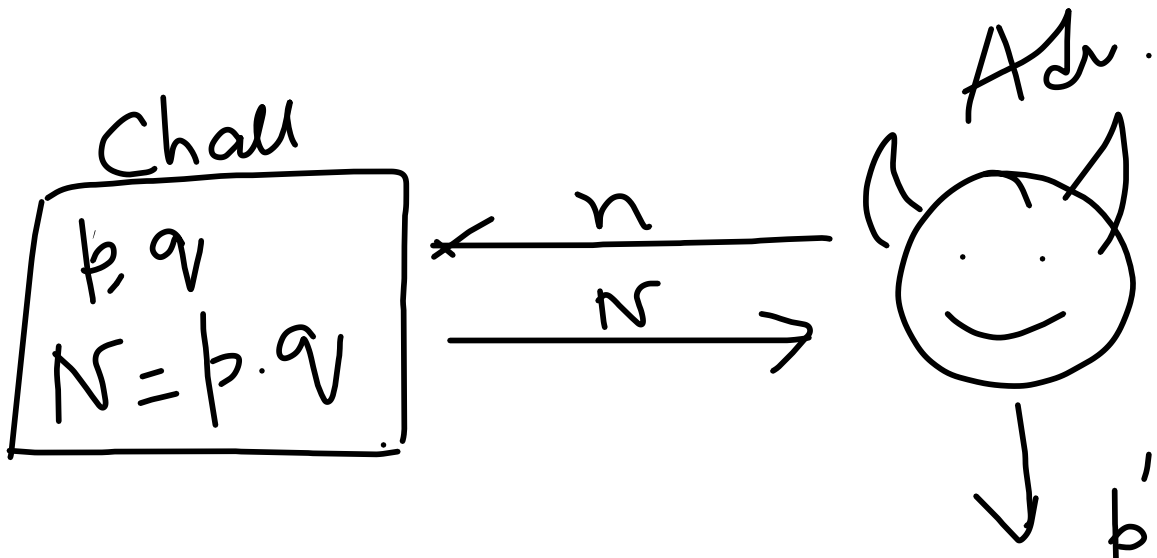
$N = pq.$ $Z_N \cong Z_p \times Z_q.$

Then what is the time complexity of finding out $f^{-1}(\alpha, \beta)$.

Where f is defined as $f(x) = (x \bmod p, x \bmod q), \forall x \in Z_N.$

Factoring problem

$f_n(p,q) = p \cdot q$



$\downarrow$ p', q' s.t $N = p' \cdot q'$

p, q are distinct n bit prime numbers.

Adversary wins if $N = p' \cdot q'$

We call Factoring problem is hard if the winning prob. of any prob. poly time adv. of this game is negligible fn w.r.t. to n.

We assume that factoring is a hard problem $\longrightarrow$ Factoring assumption.

Factoring assumption yields a one way fn but it can't be used in this form in cryptographic application.

RSA assumption: Suppose p and q are n-bit primes and $N = pq$. We consider the group $\mathbb{Z}_N^*$ of order

$$\phi(N) = (p-1)(q-1).$$

- If the factorization of N is known, then computing the order of $\mathbb{Z}_N^*$ is easy.

- If the factorization of N is unknown, then it is difficult to compute $\phi(N)$. — justify this

Contrapositive, if computing $\phi(N)$ is easy, then we can find out the factors of N in poly time.

RSA assumption exploits this asymmetry.

RSA problem is easy to solve when $\phi(N)$ is known.
but appears hard to solve without the knowledge of $\phi(N)$.

RSA problem

Given a modulus N and an integer $e > 0$ such that $\gcd(e, \phi(N)) = 1$ and an element $y \in \mathbb{Z}_N^*$ compute $y^{1/e} \bmod N$.

Suppose consider a fn. $f: \mathbb{Z}_N \to \mathbb{Z}_N$.

$f_{N,e}(x) = x^e \bmod N$ where $N = p \cdot q$, p, q are distinct primes and $e > 0$ s.t $\gcd(e, \phi(N)) = 1$.

Prove $f_{N,e}$ is a permutation.

Consider x_1, x_2

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

$f(x_1) = x_1^e \bmod N.$

$f(x_2) = x_2^e \bmod N.$

$x_1^{ed} \bmod N.$

$\Rightarrow x_1^{1+k\phi(N)} \bmod N.$

$= x_1 \cdot \underbrace{\left(x_1^{\phi(N)} \bmod N\right)^k}_{1}$

$ed = 1 + k\phi(N).$

$\Rightarrow$

$f_{N,e}(x) = x^e \bmod N.$

$y = x^e \bmod N.$

$f_{N,d}(y) = y^d \bmod N.$

$f_{N,d}(f_{N,e}(x)) = x.$

$= f_{N,d}(x^e \bmod N) = x^{ed} \bmod N$

$x^{ed} \bmod N$

Since $ed = 1 + k\phi(N)$

$= 1 + k(p-1)(q-1)$.

$x^{1+k(p-1)(q-1)} \bmod N$.

$(0, 2)$

CRT $x \longleftrightarrow (x_p, x_q) = (x \bmod p, x \bmod q)$.

$x^{1+k(p-1)(q-1)} \longleftrightarrow \left(\underbrace{x^{1+k(p-1)(q-1)} \bmod p}, \right.$

$\left. x^{1+k(p-1)(q-1)} \bmod q \right)$.

$= (x, x) = x(1, 1) = x$

$RSA\text{-}Inv_{A, GenRSA}(n)$

1. Run $GenRSA(1^n)$ to obtain (N, e, d)
2. choose $x \leftarrow\$ \mathbb{Z}_N$ and compute $x^e \bmod N$
3. A is given $N, e, x^e \bmod N$ and o/p $x' \in \mathbb{Z}_N$
4. output 1 if $x = x'$

$e = 3$

$x < N^{1/3}$

We say that RSA problem is "hard" if $\forall$ PPT alg. A.

$$Pr\left[RSA\text{-}inv_{A, GenRSA}(n) = 1\right] \leq negl(n)$$

$x^3 \bmod N$

$C = x^3 \bmod N$

$C^{1/3}$

RSA assumption is simply the assumption that ∃ a GenRSA module relative to which the RSA problem is hard.

GenRSA

Input: Security param. n

Output: (N, e, d)

$(N, p, q) \leftarrow$ GenModulus (1^n)

$\phi(N) := (p-1)(q-1)$.

find $e > 0$ s.t. $\gcd(e, \phi(N)) = 1$

Compute $d = e^{-1} \bmod \phi(N)$.

return (N, e, d).

GenModulus (1^n)

Input: security param. n.

Output: (N, p, q)

- Randomly samples $p, q \in \{0,1\}^n$
- check whether p and q are prime or not.
- if they are prime, compute $N = p \cdot q$.
- return (N, p, q).