The RSA Cryptosystems (8)

Correctness of RSA

$N = PQ$, $ED \equiv 1 \pmod{(P-1)(Q-1)}$

Assume GCD(X,N)=1. By **Fermat's Little Thm**,

$$X^{(P-1)(Q-1)} \equiv (X^{P-1})^{Q-1} \equiv 1 \pmod{P}$$

$$X^{(P-1)(Q-1)} \equiv (X^{Q-1})^{P-1} \equiv 1 \pmod{Q}$$

$$\Rightarrow X^{(P-1)(Q-1)} \equiv 1 \pmod{N=PQ}$$

Since $ED = 1 + K(P-1)(Q-1)$,

$$(X^E)^D \equiv X \times (X^{(P-1)(Q-1)})^K \equiv X \pmod{N}.$$

The RSA Cryptosystems (9)

Possible attack to RSA

- Can we recover the **plaintext** X (mod N) from E and the **ciphertext** $Y \equiv X^E \pmod N$?
- **Assume** we calculate N=PQ.
  Then we can calculate D
  s.t. $ED \equiv 1 \pmod{(P-1)(Q-1)}$.
- People believe **Integer Factorization** is a difficult problem if P,Q are large.