The RSA Cryptosystems (6)

RSA Key Generation

- **$P \neq Q$** large prime numbers, **N** $= PQ$
- Choose random $1 < \mathbf{E} < (P-1)(Q-1)$
  s.t. E and $(P-1)(Q-1)$ are relatively prime.
  $\Rightarrow 1 < \mathbf{D} < (P-1)(Q-1)$ multiplicative
  inverse **$ED \equiv 1 \pmod{(P-1)(Q-1)}$**
- After that, P,Q should be discarded safely.

We will **only use N,E,D** in the cryptosystem.

The RSA Cryptosystems (7)

- **N**(=PQ), **E** are public. (E is **Public Key**.)

RSA Encryption (**E** is **Encryption Key**.)

- The **plaintext** is $0 \le \mathbf{X} \le N-1$.
- The **ciphertext** is $\mathbf{Y} \equiv X^E \pmod{N}$.

⇩

RSA Decryption (**D** is **Decryption Key**.)

- From the **ciphertext** **Y**,
  calculate $\mathbf{Z} \equiv Y^D \pmod{N}$. Then $\mathbf{Z=X}$.