Cryptography: basic concept

- Cryptography
  - Art of secret writing
  - Act of writing in code or cipher
- Cryptology/Cryptanalysis
  - Science of analyzing and deciphering codes and ciphers and cryptograms
- Two common types of cryptosystems:
  - Symmetric
  - Asymmetric

Cryptosystem

- Basic idea: Keeping secret of the information through mathematical transformation known as encryption.
- Two components: Coding algorithm + secret key(s)
- Coding is easy on one direction
- Decoding is hard without the secret keys
- Coding algorithms are made known
- Key(s) is/are kept secret for confidentiality

Two types of encryption

- **Symmetric**: often referred to as *conventional cryptography*, defined as:

$$P = D_k (E_k (P))$$

  - *Only one secret key is involved.*
- **Asymmetric**:often referred to as *public-key cryptography*, defined as:

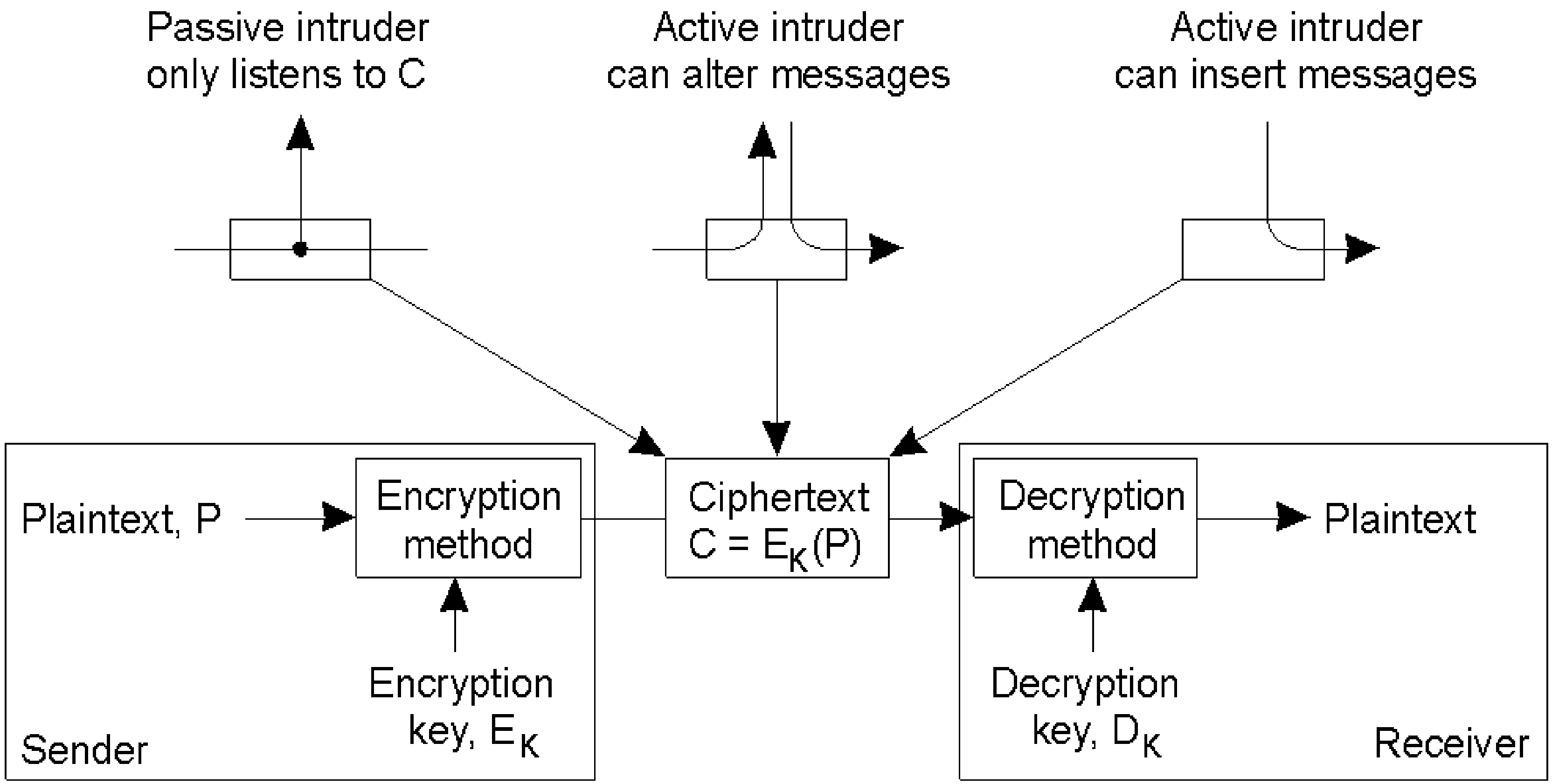
$$P = D_{k_d} (E_{k_e} (P))$$

  - Public-private key pair. Use public key for encryption, private key for decryption.
  - Private key is kept as the secret.

Hash (one-way) function

- *Hashing a message m using a hashing function H results in the hash value*
  - $h = H(m)$
- *Given H and m, h is easy to compute.*
- *Inverse of H is computationally difficult. (That's why it's a one-way function!)*
- *If H is chosen carefully to avoid collision, h could serve the purpose of signature signing.*

Participants/Components



- Intruders and eavesdroppers in communication.

Public-Key Cryptosystem: RSA

- Generating the private and public key requires four steps:
- Choose two very large prime numbers, P and Q.
- Compute *n* = *PQ* and *z* = *(P – 1)* x *(Q – 1).*
- Choose a number D that is relatively prime to *z.*
- Compute the number E such that E*D = 1 mod z.*
- *(E,PQ) is the public key, D is the private key.*
- *Encryption function: encrypt(T)=(T^E) mod PQ*
- *Decryption function: decrypt(C)=(C^D)mod PQ*

RSA: an example

An Example of the RSA Algorithm

P = 7 <- first prime number (destroy this after computing E and D)

Q = 11 <- second prime number (destroy this after computing E and D)

PQ = 77 <- modulus (give this to others)

E = ? <- public exponent (give this to others) E is chosen to be relatively prime to (P-1)(Q-1)

D = ? <- private exponent (keep this secret!)

D is chosen such that (E*D) -1 is divisible by (P-1)(Q-1) or ED = 1 mod [(P-1)(Q-1)]

RSA: an example

P=7, Q= 11 n= PQ = 77
(P-1)(Q-1)= 60

E is relatively prime to 60,
since factors of 60 is 2,3,4,5,6,10,12,15,20,30, therefore, find e such that it has no factor of factors of 60; e.g., E = 7, 11 ...

Find d such that E*D - 1 is divisible by 60

I.e., find integer D such that E*D = 61, 121, 181, 241, 301, 361, ...

RSA: an example

Now we can choose E = 11, D = 11.

Suppose Message M = 12 => Encrypted message = 45

Encryption function C = (M^E) mod PQ

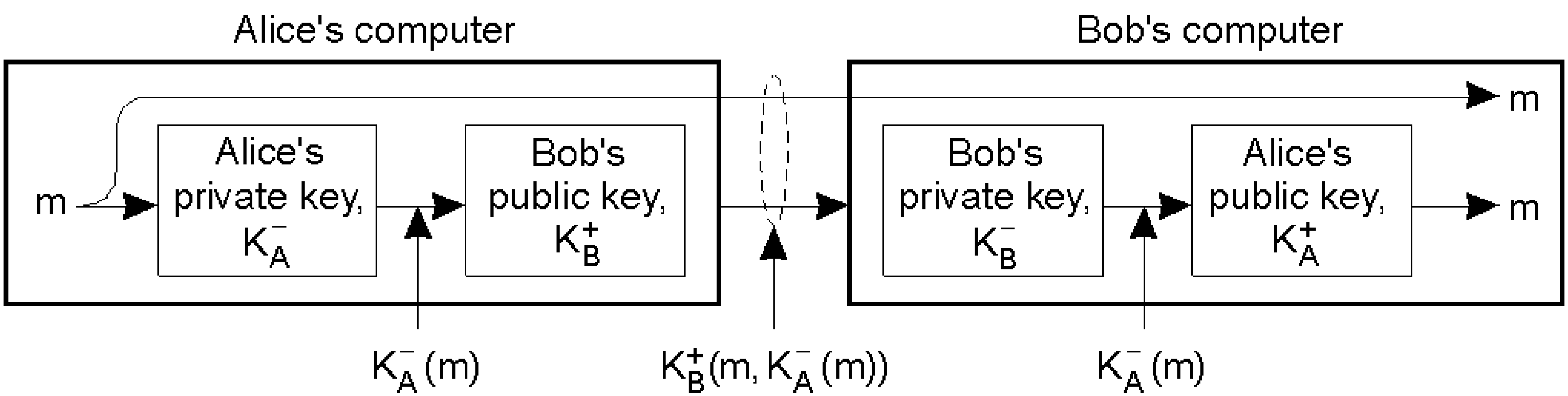
Decryption function T = (C^D) mod PQ = [(M^E) mod PQ]^D mod PQ

C = (12^11) mod 77 = 45 (or 12^11 = 77*9649459359 + 45)
(12^11)/77=9649459359.58441558441558441558 44

T = (45^11) mod 77 = 12 (or 45^11 = 77*198997181976714 69 + 12)
(45^11)/77=19899718197671469.155844155844156

Public key (pq, e)
Private key is "d"   "e" is public exponent

Digital signature



- Digital signing a message using public-key cryptography.
- This is implemented in the RSA technology.
- Question: How do we get the message m from sender to receiver for a verification?