Lecture 10: Encryption

How messages being sent?

- Packet switching via many routers.
- Routers sitting between source and destination computers can access the content of the packets.
- To ensure the privacy of the message, the text can be encrypted.

Cryptography and Cryptanalysis

- Cryptography – study of methods to encrypt text.
- Cryptanalysis – study of how to decode an encrypted text.

Conventional encryption

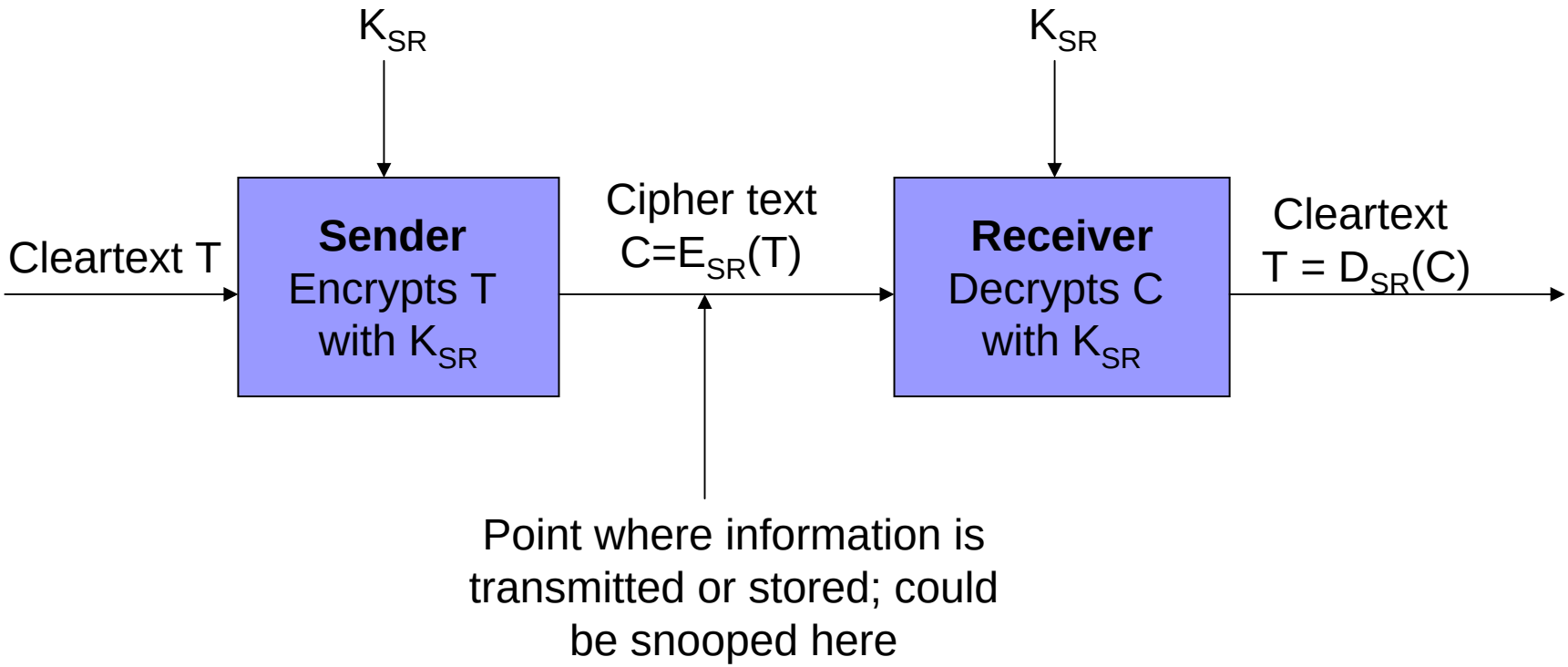
- Conventional encryption or single key encryption – a simple algorithm is used to transform the clear text into encrypted text.

Substitution cipher

- Substitution cipher – each letter of the alphabet is substituted with a different letter or symbol.
- Ceasar's method – replace every letter in the alphabet with the letter 3 away:
  - A -> D
  - B->E
  - C->F
  - …
  - X->A
  - Y->B
  - Z->C

  "CIS" will encrypted as "FLV"
- Other substitution ciphers assign random substitutions, so they are a bit harder to crack.

Schematic diagram of a cryptosystem



The Ceasar's Example

- The secrete key $K_{SR} = 3$
- The encryption algorithm: $C=E_{SR}(T) = T + K_{SR}$
- The decryption algorithm: $T=D_{SR}(C) = T – K_{SR}$

Encryption and decryption procedure

- The **sender** applies the encryption algorithm to **encrypt** the clear message using a private-key.
- The **sender transmits** the **encrypted message** to the **receiver**.
- The **receiver** uses the private-key **to decrypt** the **encrypted message** back to the **clear message**.

The key exchange problem

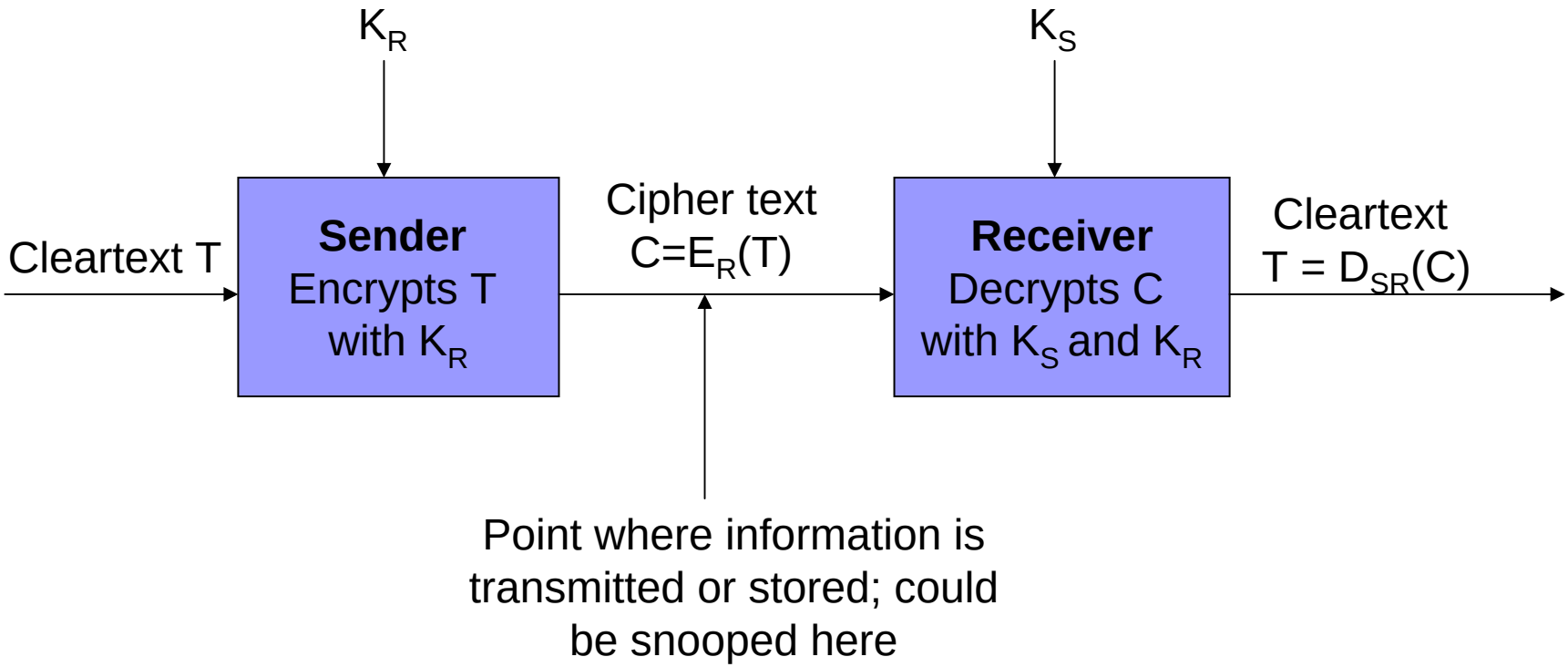
- The sender and the receiver must pre-agree on a private key ahead of time.
- They have to meet or at least communicate for the purpose of selecting the key.
- If they don’t meet, the communication to negotiate a private-key can not be made secure.
- Key exchange is a stopper for e-commerce application in Internet where the company and customer cannot meet ahead.

Public-key encryption

- Uses two keys: **public-key** and **private key**
- The receiver **publishes** a public-key.
- **The sender** uses the **public-key** to **encrypt** the clear message.
- The sender **transmits** the encrypted message to the receiver.
- **The receiver decrypt** the encrypted message using the **private-key** associating with the public-key.

Schematic diagram of a public key cryptosystem (PKC)

K_R is the public key
K_S is the secret key



Well-known public-key systems

- Elgamal – invented by Taher Elgamal
- RSA – invented by Ron **R**ivest, Adi **S**hamir and Leonard **A**delman
- DSA – Digital Signature Algorithm by David kravitz
- PGP – Pretty Good Privacy: uses both conventional and public-key cryptography

One-way trap-door function

- A **one-way function** is a function that is easy to compute, but the inverse is hard to compute.
- A **one-way trap-door function** is also a function that is easy to compute, but the inverse is hard compute; however, if **some piece of information is known (**the key**)**, the inverse becomes easy to compute as well.
  - **Encryption function** – an one-way trap-door function
  - **Decryption function** – inverse of an one-way trap-door function

The Math – An Instance of One-way Trap-door Function (RSA)

- **Public-key K_R** = p * q (where p, q are two very large prime number)
- Encryption $C=E_R(T) = T^3 \mod K_R$, namely $T^3 = K_R * t + C$, where t is the quotient of T^3 divided by K_R, and C is the reminder.
- Decryption $T = D_{SR}(C)=C^s \mod K_R$, where **$s = (1/3)(2(p-1)(q-1) + 1)$** is actually the **private-key**

Why a one-way trap-door function?

- $T^3 = K_R * t + C$, T is the clear text, and C is the encrypted text
- If the code cracker had the quotient t and the remainder C, he or she could simply
  - multiply the quotient by the key $K_R * t$
  - add in the remainder C to produce T^3,
  - then find the cube root of it to obtain T.
- But the cracker only has the reminder C and K_R, it is hard to compute the clear text T.
  - **Factoring a large number is hard! It is hard to obtain p and q from K_R=p*q, where p and q are both large primes.**
- For the receiver, he has both p and q, which is a trap-door to compute T following Euler's theorem.

The Math behind: Euler's Theorem

- **Euler's theorem (1736):** Let p and q be two distinct primes, K=pq, 0 <= T < K, and r >0. If $T^{r(p-1)(q-1)+1}$ is divided by K, the remainder is T.
- In the above PKC cryptosystem, r is set to 2:
  - $(T^3)^s = (T^3)^{(1/3)[2(p-1)(q-1) + 1]}$
    $= T^{2(p-1)(q-1) + 1}$
  - $(T^3)^s = (K_R * t + C)^s = K_R * (\ldots) + C^s$, therefore **$C^s$ mod K_R = $(T^3)^s$ mod K_R = T**
- Reminder: A **prime number** (or a **prime**) is a natural number that has exactly two (distinct) natural number divisors, which are 1 and the prime number itself.

PGP - Pretty Good Privacy

- At the sending end:
  1. PGP compresses the message to save transmission time and increase the security
  2. PGP creates a session key that is used only once during this transmission session. It is created from randomly selected mouse movements and keystrokes.
  3. Session key is used to conventionally encrypt the message.
  4. The receiver's public key is used to encrypt the session key.
  5. The encrypted message and encrypted session key are sent to the receiver.
- At the receiving end:
  1. Receiver uses private key to decrypt the session key.
  2. The session key is used to decrypt the encrypted message.
  3. The text is decompressed.
  4. Session key is discarded.
- Advantages:
  - Only a very small content is publicly encrypted
  - The session key is used just once – hard to decode by repeated attacks
  - Conventional encryption is roughly 10,000 times faster than the public-key encryption.

Summary

- Conventional encryption, single key encryption
- Public-key encryption
- RSA: depend on Euler's theorem and the difficulty of large number factoring
- One-way trap-door function
- PGP – combination of single key encryption and public-key encryption