Network Security

2. Classical Encryption Techniques

Outline

- Basic Concepts
- Types of Encryption
- Classical Encryption Techniques

Cryptography

- Concerned with developing algorithms which may be used to:
  - Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
  - Verify the correctness of a message to the recipient (authentication)

Cryptanalysis

- The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key
  - Also called code breaking
- People who do cryptography are cryptographers, and practitioners of cryptanalysis are cryptanalysts

Cryptology

- Cryptology is the branch of mathematics that studies the mathematical foundations of cryptographic methods.
- Cryptology comes from the Greek words Kryptos, meaning hidden, and Graphen, meaning to write. Cryptology is actually the study of codes and ciphers.
- Cryptology = both cryptography and cryptanalysis

Normal Encryption Process

- A message in its original form (plaintext) is encrypted into an unintelligible form (Ciphertext) by a set of procedures known as an encryption algorithm and a variable, called a key; and the Ciphertext is transformed (decrypted) back into plaintext using the encryption algorithm and a key.

Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

Concepts

- If P is the plaintext, C is the ciphertext,

Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

- E_K is chosen from a family of transformations known as a cryptographic system.
- The parameter that selects the individual transformation is called the key k, selected from a key space *K*

Concepts

- A cryptographic system is a single parameter family of invertible transformations
  - E_K ; K in K : P → C
  - with the inverse algorithm E_K^{-1} ; K in K : C → P
  - such that the inverse is unique
- Usually we assume the cryptographic system is public, and only the key is secret information

Algorithm Secrecy

- Some cryptographic methods rely on the secrecy of the algorithms
- such algorithms are only of historical interest and are not adequate for real-world needs

The Key

- All modern algorithms use a key to control encryption and decryption; a message can only be decrypted with the right key.
- The keys used for encryption and decryption can be same or different from each other.

Encryption Algorithm Types

- There are two classes of key-based algorithms:
  - **Symmetric (or secret-key)**
    - use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key)
  - **Asymmetric (or public-key)**
    - use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key

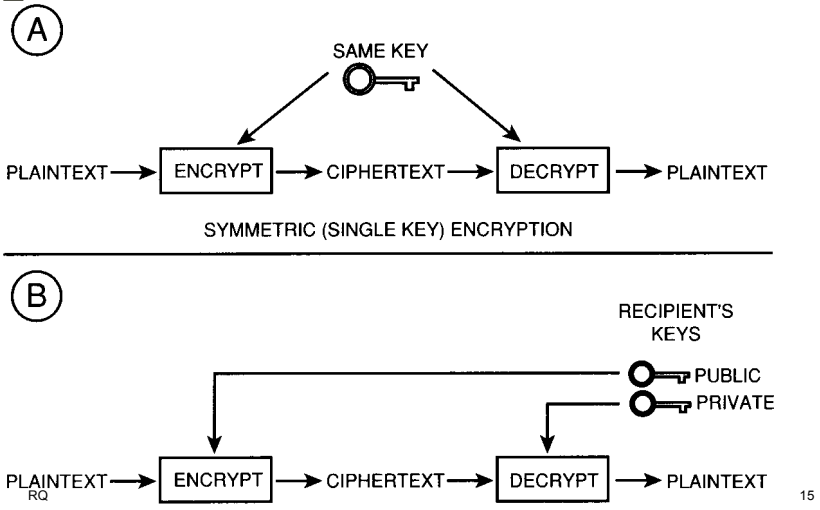
Symmetric Algorithms

- Symmetric algorithms can be divided into stream ciphers and block ciphers.
- Stream ciphers can encrypt a single bit of plaintext at a time, whereas
- Block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.

Asymmetric Algorithms

- also called public-key algorithms or generally public-key cryptography
- permit the encryption key to be public, allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message. The encryption key is also called the public key and the decryption key the private key or secret key.

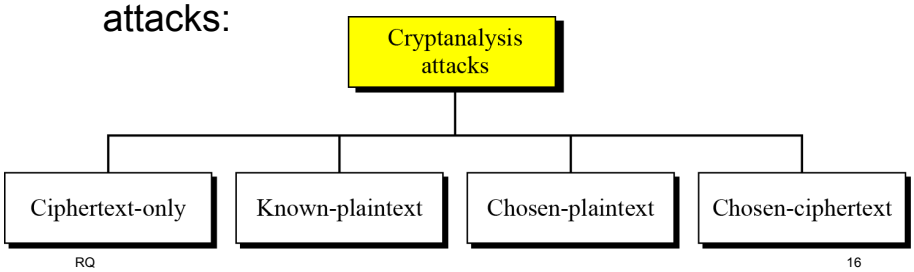
Comparison of SE and AE



RQ 15

Cryptanalysis

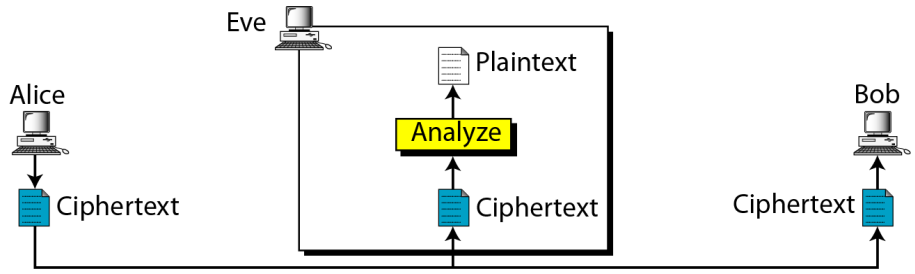
- As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes.
- There are four common types of cryptanalysis attacks:



RQ 16

Ciphertext-Only Attack

- The adversary (Eve) has access to some ciphertext and tries to find the corresponding key and the plaintext



Ciphertext-Only Attack

- Brute-Force Attack
  - Try to use all possible keys
- Statistical Attack
  - Use inherent language characteristics
- Pattern Attack
  - Make use of patterns in the ciphertext

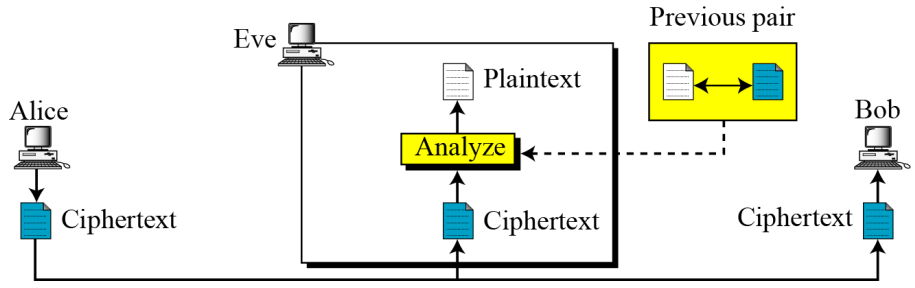
Ciphertext-Only Attack

- Brute-Force Attack
  - always possible to simply try every key
  - attack proportional to key size

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

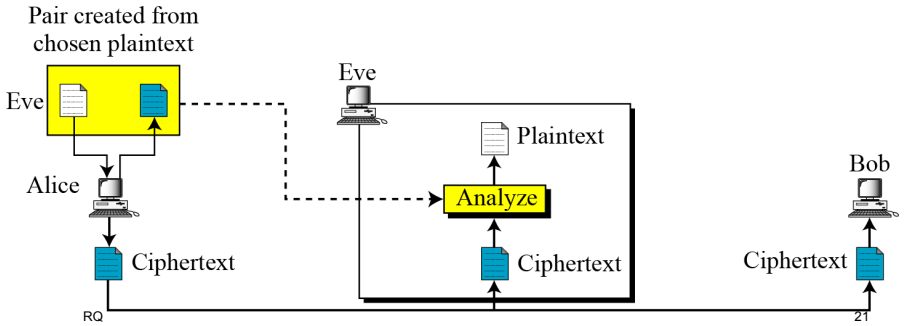
Known-Plaintext Attack

- Use known plaintext/ciphertext pair to attack new ciphertext



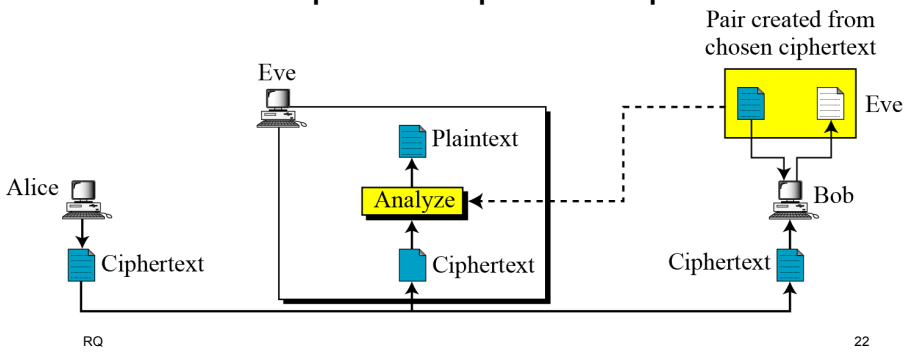
Chosen-Plaintext Attack

- Similar to known-plaintext attack but the plaintext/ciphertext pair is chosen by attacker



Chosen-Ciphertext Attack

- Similar to chosen-plaintext attach but the attacker choses ciphertext and decrypts it to form ciphertext/plaintext pair



Symmetric Encryption

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970's

Symmetric Cipher Model