Overview

密碼學與應用

海洋大學資訊工程系

丁培毅

Course Information

Course materials:
http://squall.cs.ntou.edu.tw/CryptoIntro/

Basic course contents:
Fundamental cryptography and its applications in constructing secure information infrastructure: networking environments, distributed computing resources, cloud services, and computing facilities.

Overview of Cryptography

- People want and need **privacy** and **security (confidentiality, integrity, authenticity, and availability)** while communicating
- In the past, cryptography is heavily used for military applications to keep sensitive information secret from enemies (adversaries).
  - Julius Caesar used a simple shift cipher to communicate with his generals in the battlefield.
  - World War I, World War II (Enigma)

Overview of Cryptography

- Nowadays, with the fast technologic progress, our dependency on computer systems and networks has increased a lot such that we need more sophisticated techniques to ensure the smooth operations.
- Cryptography provides most of the methods and techniques for secure communication and secure computing

Terminology

- **Cryptology:** A term used for the study of secure mechanisms for communication over insecure channels and related problems.
- **Cryptography:** The process of designing systems to realize secure communications over insecure channels.
- **Cryptoanalysis:** The discipline of breaking cryptographic systems.

Terminology

- **Coding Theory:** Deals with representing the information using codes. It covers: compression, secrecy, and error-correction.
  - Recently, it is predominantly associated with error-correcting
  - codes which ensures the correct transmissions over noisy-channels.

The Aspects of Cryptography

- Modern cryptography heavily depends on mathematics and the usage of digital systems.
- It is an inter-disciplinary study of basically three fields:

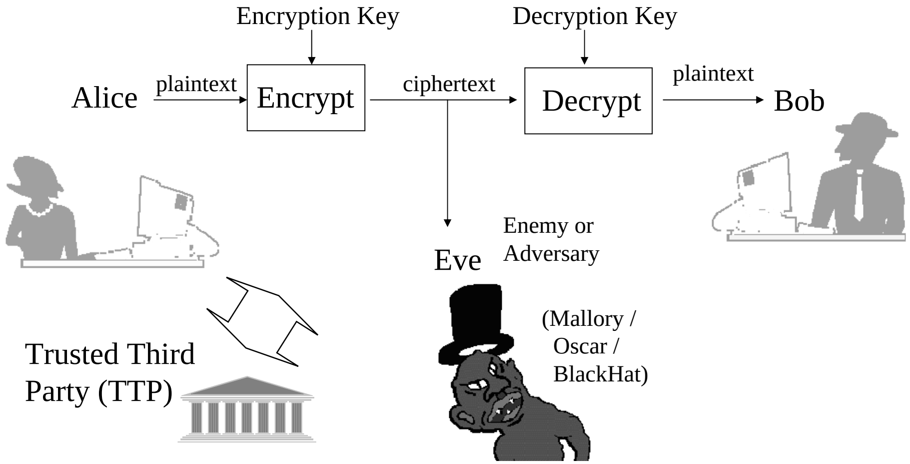
  Mathematics
  Computer Science
  Electrical Engineering

The Aspects of Cryptography

- Without having a complete understanding of cryptoanalysis / cryptoanalytic techniques / provable security, it is impossible to design *good* (secure, unbreakable) cryptographic systems.

- It makes use of other disciplines such as number theory, quantum physics, error-correcting codes, and computation theory.

Basic Communication Scenario



Eve's Goals

(1) Peep the transmitted message.

(2) Figure out the key Alice is using and read all the messages encrypted with that key.

(3) Modify the content of the message in such a way that Bob will think Alice sent the corrupted message.

(4) Impersonate Alice and communicate with Bob who thinks he is communicating with Alice.

Eve's Goals (cont'd)

- Eve or Oscar is a **passive** observer who tries to perform (1) and (2).
- Mallory is more **active** and evil who tries to perform (3) and (4).

Network Security Attacks

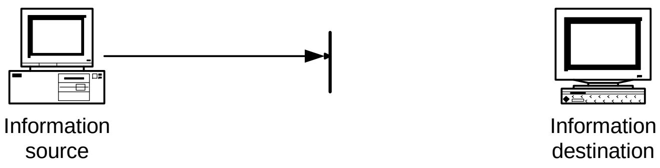
Security attack: any action that compromises the security of information

Four general categories of attacks: [W. Stalling]

- ➢Interruption
- ➢Interception
- ➢Modification
- ➢Fabrication

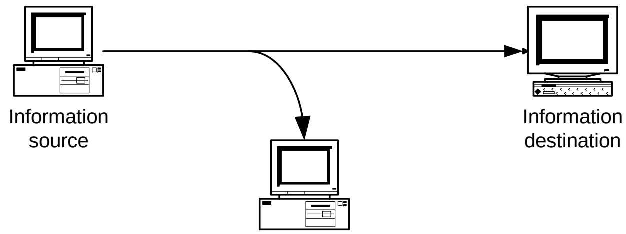
Interruption

- An asset of the system is destroyed or becomes unavailable or unusable
- This is an attack on **availability**



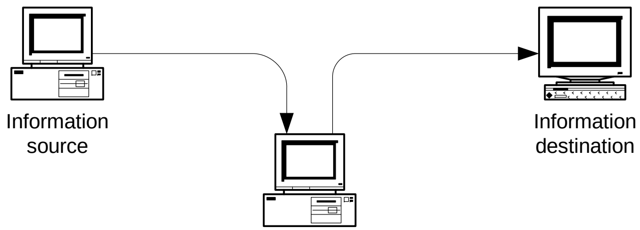
Interception

- An unauthorized party gains access to an asset
- This is an attack on **confidentiality**



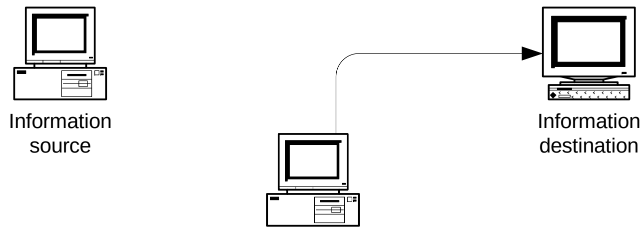
Modification

- An unauthorized party not only gains access to but tampers with an asset
- This is an attack on integrity&authenticity



Fabrication

- An unauthorized party inserts counterfeit objects into the system
- This is an attack on authenticity



Categories of Network Attacks

- Passive vs. Active

network security examples:

- **Passive threats**
  - Reveal of message contents (Eavesdropping)
  - Traffic analysis
- **Active threats**
  - Masquerade (spoofing, hijacking)
  - Replay (capture)
  - Modification of message contents (tampering)
  - Denial of service (interruption)

Classes of S/W Security Vulnerabilities

- Buffer Overflow / Underflow, Integer Overflow
- Format Strings
- Tainted Input / Input Validation
- Race Conditions
- Trust Management
- Password Management
- Database Access (user ID/password)
- Insecure temp file usage, broken CGI practices
- Poor Cryptography Practices
- Poor Randomness

Methods of Cryptoanalysis

focus on the Encrypt/Decrypt algorithm only

- **Ciphertext only:** Alice has only a copy of ciphertext
- **Known Plaintext:** Eve has a bunch of ciphertexts and the corresponding plaintexts and tries to break a particular ciphertext.

  Ex: fixed letter head:
  Dear Sir,
  fixed file format:
  <html>…..

Methods of Cryptoanalysis(cont'd)

- **Chosen Plaintext:** Eve has a copy of ciphertext corresponding to a copy of plaintext selected by Eve who believes it is useful in breaking a ciphertext. Eve can temporarily access the encryption engine.
  Ex: fighter plane transponder
  challenge - response
- **Chosen Ciphertext:** Eve has a copy of plaintext corresponding to a copy of ciphertext selected by Eve who believes it is useful in breaking a ciphertext. Eve can temporarily access the decryption engine.
  Ex: auto email response system

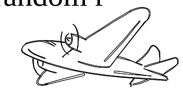
Methods of Cryptoanalysis(cont'd)

- fighter plane transponder

generate random r

r

$E_k(r)$



$D_k(E_k(r))$? r

- CPA:

r_1 r_2 r_3 ∘ ∘ ∘

∘ ∘ ∘ c_3 c_2 c_1

Kerckhoffs's Principle (1883)

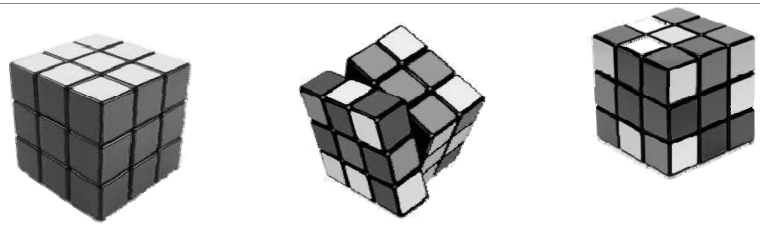
"Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvenient tomber entre les mains de l'ennemi."

([A cipher] must not depend on secrecy, and it must not matter if it falls into enemy hands.) ← obscurity of the algorithm

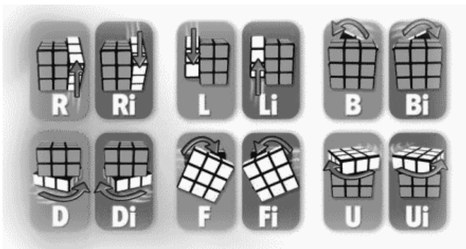
August Kerckhoffs, La Crytographie Militaire, Jan. 1883

- While assessing the strength of a cryptosystem, one should always assume that the enemy knows the cryptographic algorithm used.
- The security of an encryption system should based on
  - the quality (strength) of the algorithm but not its obscurity
  - the key space (or key length)

Kerckhoffs's Desiderata



Conceptually:
① choices of moves
② difficult to resolve the choices reversely
③ difficult to solve in a brute-force way



Security Services

- Confidentiality
- Authentication
- Integrity
- Non-repudiation
- Access control (Identification)

Symmetric & Public Key Algorithms

- **Symmetric Key Cryptosystems**
  - Encryption and decryption keys are known to both communicating parties (Alice and Bob).
  - They are usually related and it is easy to derive from each other (i.e. easy to derive the decryption key once one knows the encryption key and vice versa).
  - In most cases, they are identical.
  - All of the traditional (pre-1970) cryptosystems are symmetric.

Also known as secret-key cryptosystem

Symmetric Key Cryptosystems

- Examples :
  - DES (Data Encryption Standard, 1976) and
  - AES (Advanced Encryption Standard, 2001): Rijndael
- A secret should be shared (or agreed) between communicating parties.

Public Key Cryptography (PKC)

- **Why public key cryptography ?**
  - Key distribution and management are difficult in symmetric cryptosystems (DES, 3DES, IDEA, AES(Rijndael)) over large networks
  - Can not provide public verifiable and non-repudiable "digital signature" with symmetric ciphers
- Public key cryptography provides functions for all security services.
- Also makes it simple to implement key exchange, secret sharing functions, etc.

Public Key Cryptosystems

- Each user has a pair of keys which are generated together under a scheme:
  - Private Key - known only to the owner
  - Public Key - known to anyone in the systems with validity assurance
- **Encryption with PKC:**
  - Sender encrypts the message by the *Public Key* of the receiver
  - Only the receiver can decrypt the message by her/his *Private Key*

asymmetry

Non-mathematical PKC the padlock metaphor

- Bob has a box and a padlock which only he can unlock once it is locked.
- Alice want to send a message to Bob.
- Bob sends his box and the unlocked padlock to Alice.
- Alice puts her message in the box and locks the box with Bob's padlock and sends the box to Bob thinking that the message is safe since only Bob can unlock the padlock and accesses the contents of the box.
- Bob receives the box, unlocks the padlock and reads the message.

Non-mathematical PKC

- **Attack:**
  – Eve can replace Bob's padlock with hers when Bob is sending the box and padlock to Alice.

Simple Puzzle

- 腐敗的俄羅斯郵政系統
  – 任何有價值,未上鎖的東西在經過郵政系統傳遞時安全抵達目的地的機會很接近 0
  – 聰明的俄羅斯人當然有辦法對付
  – Question: 有一個有爲的青年要送給他的女友一枚貴重的戒指,他有一個很堅固的的鐵盒,可以用鎖頭鎖住, 請問他和他的女友該如何配合而可將戒指安全地寄達??

Shamir's three pass protocol

Problems of PKC

- Powerful tools with their own intrinsic problems.
  – **Computationally intensive** operations are involved. Much slower than the symmetric key algorithms. PKC should not be used for encrypting large quantities of data.
  – Implementation is always a challenge.

Example PKCs

- RSA
- Rabin
- Discrete Logarithm based cryptosystems. (ElGamal)
- Elliptic Curve Cryptosystems
- Goldwasser-Micali
- Paillier
- Ajtai-Dwork
- Merkel-Hellman (Rivest-Chor)
- Cramer-Shoup

Secret-Key vs Public-Key Systems

- Secret Key System offers
  - Information Secrecy (Privacy, Confidentiality)
  - Authentication (assuring that the other principal is the one who knows the shared key)
  - Integrity (using MAC)
- Disadvantages of a Secret Key System
  - key distribution/ key exchange
  - # of keys (key management)
  - can not offer non-repudiation

Secret-Key vs Public-Key Systems (cont'd)

- Public Key System offers
  - information secrecy
  - key distribution / key management
  - non-repudiation
  - authentication and integrity
- Disadvantages of a Public Key System
  - **slow**, ex. RSA is 1000 times slower than DES (about 10^{-4} sec on a PIII 800 PC)
- Simple Designs
  - **cryptosystem** $D_{k_2}(E_{k_1}(m)) = m$ • **signature system** $E_{k_1}(D_{k_2}(m)) = m$
  - not every public key algorithm can be designed as both a cryptosystem and a signature system in this way, unless Encryption and Decryption algorithms are commutable

Key Length in Cryptosystems

- Following the Kerckhkoffs's Principle, the security of cryptosystems based on
  - the quality of the algorithm
  - the key length
- The quality of cryptographic algorithms is hard to measure (requires cryptanalysis)

Key Length in Cryptosystems

- However, the key space should be large enough to prevent the adversary to determine the key simply by trying all possible keys in the key space.
- This is called **brute force** or **exhaustive search attack.**
- For example, DES utilizes 56-bit key, therefore there are 2^{56} (or approx 7.2 x 10^{16}) possible keys in the key space

Key Length in Cryptosystems

- Assume that there are 10^{30} possible key you need to try and you can only try 10^{9} key in a second.
- Since there are only around 3x10^{7} seconds in a year, brute force attack would take more than 3x10^{13} years to try out the keys. This duration is longer than the predicted life of the universe.

Key Length in Cryptosystems

- For a cryptanalyst, brute-force should be the last resort.
- S/He needs to take advantage the weakness <u>in the algorithm</u> or <u>in the implementation</u> of the cipher in order to reduce the possible keys to try out.
- Longer keys do not necessarily improve the security

NSA Suite-B: Security Strength of Practical Algorithms

Security Strength (bits)	**Symmetric Key**	**Asymmetric Key**	**Elliptic Curve Asymmetric Key**	**Message Digest**
80 (too weak by 2010)	Triple DES (2 key)	1024-bit RSA / DSA	160-bit ECDSA	SHA-1
112 (too weak	Triple DES (3 key)	2048-bit RSA / DSA	224-bit ECDSA	SHA-224
by 2030) 128	128-bit	3072-bit RSA / DSA	256-bit ECDSA	SHA-256
192	AES 192-bit	7680-bit RSA / DSA	384-bit ECDSA	SHA-384
256	AES 256-bit	15360-bit RSA / DSA	512-bit ECDSA	SHA-512

AES

Large Numbers

Physical Analogue	Number
Odds of being killed by lightning (per day)	1 in 9 billion (2^{33})
Odds of winning the top prize in a US state lottery	1 in 4,000,000 (2^{22})
Odds of winning the top prize in a US state lottery and being killed by lightning in the same day	1 in 2^{55}
Odds of drowning in the US per year	1 in 59,000 (2^{16})
Odds of being killed in an automobile accident in the US (in 1993)	1 in 6100 (2^{13})
Odds of being killed in an automobile accident in the US per lifetime	1 in 88 (2^{7})
Time until next ice age	14,000 (2^{14}) years
Time until the sun goes nova	10^9 (2^{30}) years
Age of the planet	10^9 (2^{30}) years
Age of the universe	10^{10} (2^{34}) years
Number of atoms in the planet	10^{51} (2^{170})
Number of atoms in the sun	10^{57} (2^{190})
Number of atoms in the galaxy	10^{61} (2^{223})
Number of atoms in the universe (dark matter excluded)	10^{77} (2^{265})
Volume of the universe	10^{84} (2^{280}) cm^3

Large Numbers

If the Universe is Closed:	
Total lifetime of the Universe	$10^{11}(2^{37})$ years
	$10^{18}(2^{61})$ seconds
If the Universe is Open:	
Time until low-mass stars cool off	$10^{14}(2^{47})$ years
Time until planets detach from stars	$10^{15}(2^{50})$ years
Time until stars detach from galaxies	$10^{19}(2^{64})$ years
Time until orbits decay by gravitational radiation	$10^{20}(2^{67})$ years
Time until black holes decay by the Hawking process	$10^{64}(2^{213})$ years
Time until all matter is liquid at zero temperature	$10^{65}(2^{216})$ years
Time until all matter decays to iron	$10^{10^{26}}$ years
Time until all matter decays to black hole	$10^{10^{76}}$ years

The above data comes from Schneier's "Applied Cryptography," 1996

Key Length in Cryptosystems

Symmetric and Public-key Key Lengths with Similar Resistances to Brute-Force Attacks

Symmetric Key Length	Public-key Key Length
56 bits	384 bits
64 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

The above data comes from Schneier's "Applied Cryptography," 1996

Chinese Number Systems

- 中國古代的【孫子算經】一書中有記載：「 凡大數之法，萬萬曰億，萬萬億曰兆，萬萬兆曰京，萬萬京曰垓（讀做 ㄍㄞ），萬萬垓曰秭（讀做 ㄗˇ），萬萬秭曰穰（讀做 ㄖㄤˊ），萬萬穰曰溝，萬萬溝曰澗，萬萬澗曰正，萬萬正曰載。」
- 隨著印度佛經的傳入中國，而增加了恆河沙、阿僧祇、那由他、不可思議、無量等，這些數詞都出現在佛經中，用來計量時間的長度

Chinese Number System (cont'd)

24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
秭	千垓	百垓	十垓	垓	千京	百京	十京	京	千兆	百兆	十兆	兆	千億	百億	十億	億	千萬	百萬	十萬	萬	千	百	十	個

10^x

72	68	64	60	56	52	48	44	40	36	32	28	24	20	16	12	8	4	3	2	1	0
大數	無量	不可思議	那由他	阿僧祇	恆河沙	極	載	正	澗	溝	穰	秭	垓	京	兆	億	萬	千	百	十	個