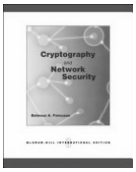
Introduction to Cryptography
SCR3443
Semester II, 2013/14

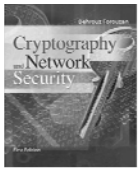
By:
Rashidah Kadir
Department of Computer Sciences
Faculty of Computing
rashidah@utm.my ☎ 07-5532414
rashidahabdkadir@gmail.com

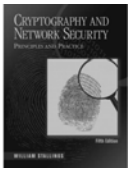
Course Learning Outcome

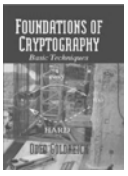
- At the end of the course, students should have the following knowledge, skills and attitude to:
  - Illustrate the fundamental concepts in cryptography.
  - Apply the necessary theory to perform encryption and decryption processes.
  - Differentiate techniques used in cryptography which relate to their different uses.
  - Recommend tools, techniques and trends cryptography for data security.
  - Formulate data security strategies using latest cryptography technique.

References









Honor Code
Collaboration on homework with other students encouraged.
However, write alone and give credit.

Information Security

- Confidentiality /Privacy
  - keeping information secret from all but those who are authorized to see it.
- Data Integrity
  - ensuring information has not been altered by unauthorized or unknown means.
  - maintaining data consistency
- Entity Authentication /Identification
  - corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.)

... Information Security

- Message authentication
  - corroborating the source of information; also known as data origin authentication.
- Signature
  - a means to bind information to an entity.
- Authorization
  - conveyance, to another entity, of official sanction to do or be something.
- Validation
  - a means to provide timeliness of authorization to use or manipulate information or resources.

... Information Security

- Access control
  - restricting access to resources to privileged entities.
  - unauthorized users are kept out
- Certification
  - endorsement of information by a trusted entity.
- Timestamping
  - recording the time of creation or existence of information.
  - Originator of communications can't deny it later

... Information Security

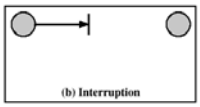
- Witnessing
  - verifying the creation or existence of information by an entity other than the creator.
- Non-repudiation
  - preventing the denial of previous commitments or actions.
- Availability
  - Legitimate users have access when they need it
- Some objectives are combined:
  - User authentication used for access control purposes
  - Non-repudiation combined with authentication

Security Threats

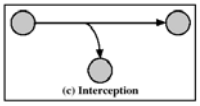
- Information disclosure/information leakage
- Integrity violation
- Masquerading
- Denial of service
- Illegitimate use
- Generic threat: Backdoors, trojan horses, insider attacks
- Most Internet security problems are access control or authentication ones
- Denial of service is also popular, but mostly an annoyance

Main Classes Of Threats

- **Interruption** - an assets is lost / unavailable / cannot be utilized eg: database is delete

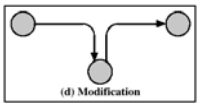


- **Interception** - an unauthorized party (person/program) has gained access to an asset eg: wiretapping

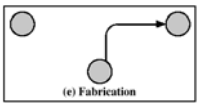


… Main Classes Of Threats

- **Modification** : an unauthorized party (person/program) has gained access and tampered around it, eg: modifying an item of database.

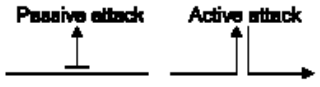


- **Fabrication**: Production of counterfeit objects for computing system, eg repeating a financial transaction



Types of Attack

- Passive attack can only observe communications or data
- Active attack can actively modify communications or data
  - Often difficult to perform, but very powerful
  - Mail forgery/modification
  - TCP/IP spoofing/session hijacking



Security Mechanism

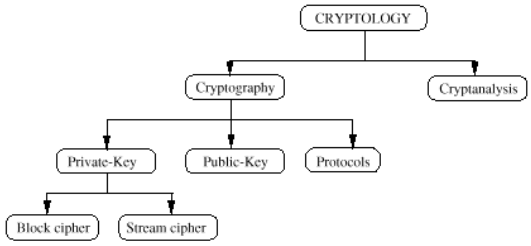
- Security Mechanism
- Physical protection
- **Cryptography**
- Access Control
- Authorization
- Auditing

Cryptography is only a small part of protection needed for "absolute" secrecy.

Cryptography

- Essential tool for making secure computing systems.
  - Badly designed protocols are easily exploited to break into computer systems, to eavesdrop on phone calls, to steal services, and so forth.
- Design is hard.
  - It is easy to under-estimate the task and quickly come up with ad hoc protocols that later turn out to be wrong.
  - the necessary time and expertise for proper protocol design is typically under-estimated, often at future cost.
  - takes knowledge, effort and ingenuity to do the job right.

Overview Field of Cryptology



Cryptography

- "Crytography is the science of secret writing." - Matt Blaze
- Cryptography is the study of secret (crypto) writing (graphy) concerned with developing algorithms which may be used to provide (goals):
  - secrecy
  - authenticate that a message has not changed in transit (integrity)
  - implicitly authenticate the sender
- Cryptography is defensive and can protect ordinary commerce and ordinary people.

Support for Security Mechanisms

- Three basic building blocks are used:
  - Encryption is used to provide confidentiality, can provide authentication and integrity protection.
- Digital signatures are used to provide authentication, integrity protection, and non-repudiation.
- Checksums/hash algorithms are used to provide integrity protection, can provide authentication
- One or more security mechanisms are combined to provide a security service.

Fundamental Idea of Cryptography

- Possible to transform plaintext into ciphertext in which information is present but hidden. We can release the transformed message without exposing the information it represent.
- Different transformations create different ciphertext for the exact same message.
- For perfect ciphers, any ciphertext can be interpreted as any message.

What Cryptography Can Do

- It can protect privacy.
  - It separates the security of a message from the security of the media.
- It can authorize someone.
- It can facilitate trust.
- It can allow for digital credentials (authentication).
- It can validate the integrity of information.
- It can ensure the fairness of financial transactions.
- It can provide an audit trail for later dispute resolution.
- Cryptography stops lying and cheating.

Other Uses of Cryptography

- More specialized uses:
  - Digital signatures
  - Undeniable digital signatures
  - All-or-nothing disclosure of secrets
  - Zero-knowledge proofs
  - Oblivious transfer
  - Simultaneous exchange of secrets
  - Secure elections
  - Digital cash

Things that Cryptography Cannot Do

- Cryptography can only hide information after it is encrypted and while it remains encrypted.
  - Secret information generally does not start out encrypted, so there is normally an original period which the secret are not protected.
  - Secret information generally is not used in encrypted form, so it is again outside the cryptographic envelope every time the secret is used.
- Cryptography cannot protect against informants, undercover spying, bugs, photographic evidence or testimony.

Adversaries

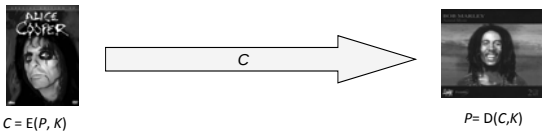
- Hackers: informal and institutional
- Insiders
- Lone criminals
- Commercial espionage
- Press
- Organized crime
- Terrorists
- National intelligence

Criminal Attacks

- "How can I acquire the maximum financial return by attacking the system?"
- Forgery, misrepresentation, replay, repudiation
- Generally opportunistic
- Minimum necessary resources
- Focuses on low-tech flaws
- Focuses on the weakest systems
- Medium risk tolerance: willing to risk job or jail time.

Components of a Cryptosystem

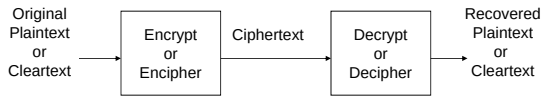
- Plaintext message space, P
- Ciphertext message space, C
- Key space, K
- A set of encryption algorithms, E_k
- A set of decryption algorithms, D_k



$C = E(P, K)$ $P = D(C, K)$

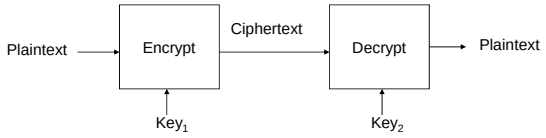
Encryption and Decryption

- Encryption
  - Process of encoding an information so that its meaning is not understood.
- Decryption
  - Process of decoding the encrypted message to get back the original information.



Keyless and Keyed Cryptosystem

- Keyless cryptosystem performs E/D without using any key.
- Symmetric key : $Key_1 = Key_2$
- Asymmetric key : $Key_1 \neq Key_2$



Algorithm E/D

- Plaintext, $P = [p_1, p_2, ..., p_n]$
- Ciphertext, $C = [c_1, c_2, ..., c_n]$
- If E and D are the encryption and the decryption algorithms respectively, then

  $C = E(P)$

  $P = D(C)$
- Cryptosystem should behave as follows:

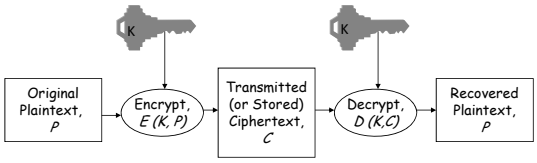
  $P = D(E(P))$ or $P = D(Key_2, E(Key_1, P))$

Features of a Good Cryptosystem

- *E* and *D* algorithms must be efficient.
- The system must be easy to used.
- The security of the system must depend on the secrecy of the keys and **NOT** on the secrecy of the *E* and *D* algorithms.
- The size of the ciphertext is not unnecessary larger than the plaintext.

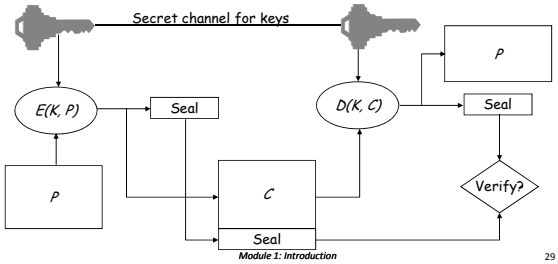
Confidentiality

- Keeping the contents of a message confidential: during transmission or storage.
- If A sends a message to B, but the enemy intercepts it, A must make sure that this enemy will never understands the content of the message.



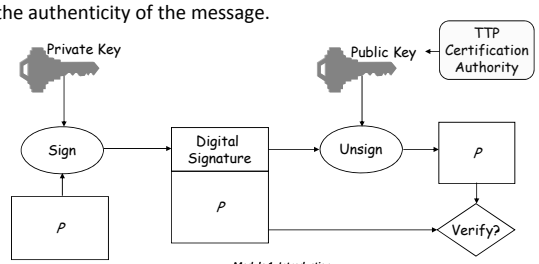
Integrity

- Proving that the contents of a message have remained unchanged.



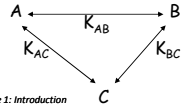
Authenticity/Non-Repudiation

- Proving that a message comes from the declared, authentic source
- Preventing an authentic source from later denying (or repudiate) the authenticity of the message.



Symmetric Key Cryptosystem

- A single key shared by both sender and receiver.
- Advantages:
  - Fast encryption/decryption process, efficient for long messages
- Weakness:
  - Requires establishment of a secure channel for key exchange.
  - If this key is disclosed, communications are compromised.
- Suppose 3 persons A, B, C want to communicate to each other in private,



Asymmetric/Public Key Cryptosystem

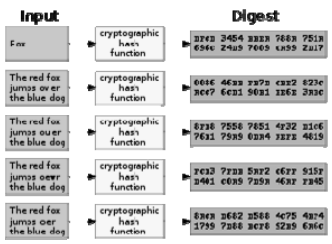
- Key that is used to encrypt the message is different to the key used to decrypt the message.
- Public key widely available - anyone wanting to send them a message uses the algorithm and the recipient's public key to do so.
- Only the recipient, with their private key can decrypt the message.
- Weakness
  - computationally intensive, encryption and decryption take longer.
  - Not suitable for encrypting long messages

Hashing

- Cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value.
- Ideal cryptographic hash function has four main or significant properties:
  - it is easy to compute the hash value for any given message,
  - it is infeasible to generate a message that has a given hash,
  - it is infeasible to modify a message without hash being changed,
  - it is infeasible to find two different messages with the same hash.

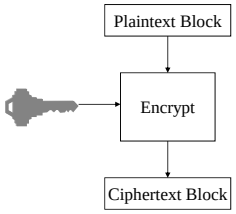
… Hashing

- A cryptographic hash function (specifically, SHA-1) at work. Note that even small changes in the source input (here in the word "over") drastically change the resulting output, by the so-called avalanche effect.



Block Cipher

- Encrypts a group of plaintext symbols as one block.
- Decryption is simply the reverse of the encryption process using the same secret key.
- Different plaintext blocks, usually 64 bits, are mapped to different ciphertext blocks; a block cipher effectively provides a permutation of the set of all possible messages.
- The actual permutation produced during any particular operation is secret, and determined by a key.



… Block Cipher

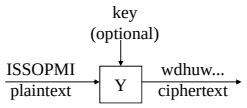
- Advantages:
  - information from the plaintext is diffused into several ciphertext symbol.
  - immunity to insertions since a single insertion into a block would result an incorrect length and thus could be detected during decryption.
- Disadvantages:
  - block cipher must wait until an entire block of plaintext has been received before starting the encryption process; this result in slowness of encryption.
  - error propagation whereby a single error will affect the transformation of all other characters in the same block.

Stream Cipher

- A stream cipher breaks the plaintext into units, normally a single character. It encrypts the *n*th unit of the plaintext with the *n*th unit of the key stream.
- Stream ciphers can be designed to be exceptionally fast.
- Each character is encrypted without regard for any other plaintext character, each character can be encrypted as soon as it is read.
- Stream cipher has low error propagation since each character is separately encoded. Error encounter only affects that particular character.

… Stream Cipher

- Run about 10 times faster than comparable block ciphers
- Disadvantages:
  - low diffusion whereby all information of that particular character of the plaintext is retained in the character of the ciphertext.
  - susceptibility to malicious insertion and modification



Cryptanalysis

- Process of attempting to discover the plaintext or the key used.
- Strategy depend on the nature of the encryption scheme and the information available.
- However, an encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine the corresponding plaintext.
- *Reading: Forouzan, pg 56 - 60*

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Ciphertext Only

- Cryptanalyst has only the ciphertext from which to determine the plaintext.
  - No knowledge whatsoever of the actual message
- The cryptoanalyst has the cipher-text of one or several messages.
  - want to recover the plaintext or (better) the key.
  - Given: $C_1 = E(P_1)$, $C_2 = E(P_2)$, ..., $C_i = E(P_i)$
  - Deduce:
    Either P_1, P_2, ..., P_i, K;
    or an algorithm to infer P_{i+1} from $C_{i+1} = E(P_{i+1})$.

Known-Plaintext Attack

- In known-plaintext attack the attacker has pairs $(x, e(x))$, but the choice of x is not under the attacker's control.

Chosen-Plaintext

- Attacker has pairs $(x, e(x))$ and x is chosen by the attacker.
  - capability to find the ciphertext corresponding to an arbitrary plaintext message of his or her own choosing.
- The likelihood of this type of attack being possible is not much.
- Codes which can survive this attack are considered to be very secure.
- Adaptive chosen plaintext attack, the cryptanalyst can determine the ciphertext of chosen plaintexts in an iterative process based on previous results. This is the general name for a method of attacking product ciphers called "differential cryptanalysis".

… Chosen-Plaintext Attack

- Want to recover the key.

  Given: P_1, P_2, ..., P_i, $C_1 = E(P_1)$, $C_2 = E(P_2)$, ..., $C_i = E(P_i)$ where we can select P_1, P_2, ..., P_i.

  Deduce: Either K or an algorithm to infer P_{i+1} from $C_{i+1} = E(P_{i+1})$.

Chosen-Ciphertext

- Cryptanalyst can choose an arbitrary ciphertext and find the corresponding decrypted plaintext.
- This attack can be used in public key systems, where it may reveal the private key.
- Chose the ciphertext to be decrypted.
  Given: C_1, C_2, ..., C_i, $P_1 = D(C_1)$, $P_2 = D(C_2)$, ..., $P_i = D(C_i)$
  Deduce: K

Breakable Cipher

- There is an algorithm known to be able theoretically break the cipher.
- A breakable cipher may not be feasible broken except by using current technology.
- Example using *brute force* which require 10^{30} operations.
- Cipher is breakable but infeasible!
- Cryptanalysis is hard, tedious, repetitive and very expensive. Success is never assured.

Kerckhoffs' Principle

- Also called Kerckhoffs' assumption, axiom or law
- State: "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."
- Majority of civilian cryptography makes use of publicly-known algorithms
  - But ciphers used to protect classified government or military information are often kept secret.
- The resistance of the cipher to attack must be based only on the secrecy of the key.
- Key domain for each algorithm is so large that it makes it difficult for the adversary to find the key.

Conclusions

- The problem with bad cryptography is that it looks just like good cryptography.
- Successful attacks are often kept secret. Unless attackers publicize.
- We need to be proactive.
  - Understand the real threats to a system
  - Design systems with strong cryptography
  - Build cryptography into systems at the beginning
- Perfect solutions are not required, but systems that can be broken completely are unacceptable.