Module 22: Multi-core Computing Security

Lecture 44: Cryptography and ECB

The Lecture Contains:

Previous Next

Cryptography

- Cryptographers: (good guys)
  - Invent clever algorithms
- Cryptanalysts: (bad guys)
  - Attempt to break algorithms
- *If lots of smart people have failed to solve a problem, then it probably won't be solved, at least in near future.*
- Cryptography systems depend upon computationally difficult problems which become simple when a secret (key) is known.

Is Algorithm Secret?

- Some believe that keeping the algorithm secret enhances its security
- Some believe that publishing the algorithm will enhance the security.
- Difficult to keep the algorithm secret
- Common practice: Commercial algorithms are public while military applications keep it secret.

Previous Next

Some Simple Ciphers

- Caesar Cipher
    - Rotation of alphabet (substitution cipher)
    - Caesar used a fixed rotation of 3. (Computer ↔*Frpsxwhu*)
    - Variant is when this rotation is variable.
- Mono-alphabetic Substitution Cipher
    - *Si spy net work, big fedjaw iog link kyxogy*

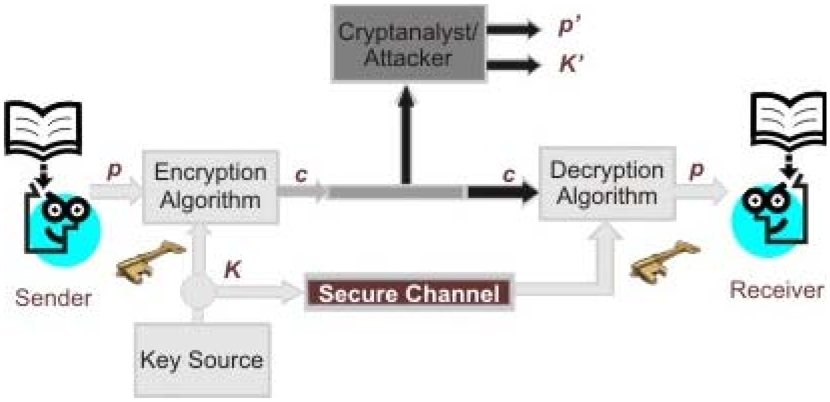
Breaking a Cipher Scheme

- Various kinds of attacks are possible.
    - Cipher-text only.
        - The attacker has access to cipher-text only but not the plaintext.
    - Known plaintext.
        - The attacker has access to few cipher-text and corresponding plaintext pairs.
    - Chosen plaintext.
        - The attacker can run his plaintext to get the corresponding cipher-text.
    - Chosen Cipher-text.
        - Same as chosen plaintext (but on the decryption algorithm)

Previous Next

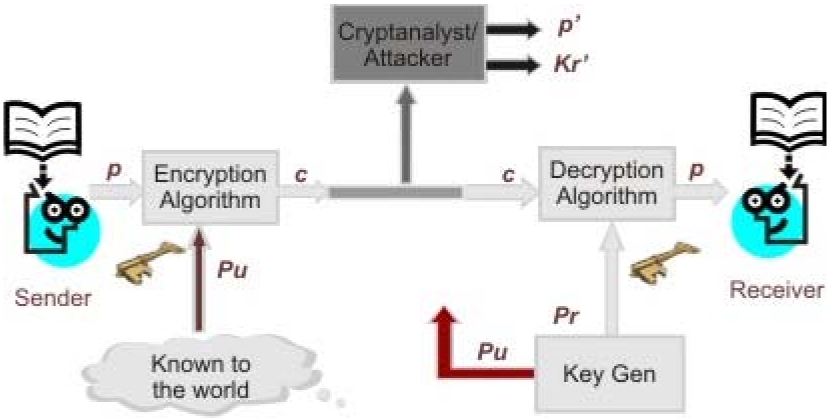
Secret Key Cryptography

- Also known as Symmetric Key Cryptography or conventional cryptography.
- The following is relevant
    - Plaintext
    - Encryption Algorithm
    - Secret Key
    - Decryption Algorithm
    - Cipher-text
- Requirements
    - Strong encryption algorithm (attackers may have access to the algorithm and a few cipher-text-plaintext pairs)
    - Sender and receiver must have access to the secret key.



Previous Next

Asymmetric Key Cryptography



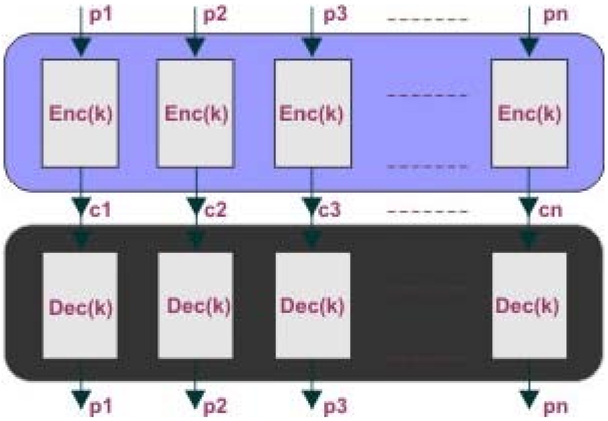
Encrypting a Large Message

- If the message is more than the size of the block, the message can be broken in multiple blocks.
- Let the message be known as concatenation of p1, p2, p3, …, pn.
- There are the following modes of operation
    - Electronic Code Book (ECB)
    - Cipher Block Chaining (CBC)
    - Cipher Feedback Mode (CFB)
    - Output Feedback Mode (OFB)
    - Counter Mode (CTR)

Previous Next

Lecture 44: Cryptography and ECB

ECB Mode of Operation



Threats on ECB Operational Mode

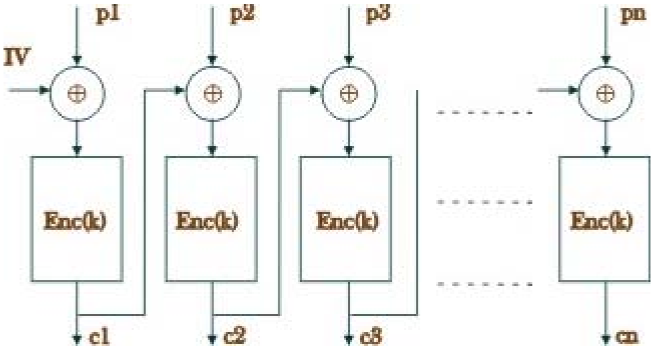
- If the message contain two identical blocks, the corresponding cipher blocks are also identical.
  - Eavesdropper gets some information.
- Consider data base rows being sent from one end to another
  - Columns: Name, Position, Salary
  - Each is 64 byte wide (block size: 64 bytes)
- Now the eavesdropper can find out
  - Number of people at a particular position
  - Number of people at the same salary.

Threats on ECB

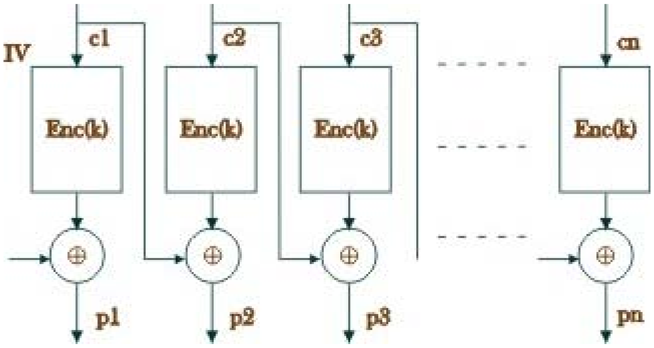
- An employee can even alter the message to change his own salary.
- Serious flaws:
  - Some one looking at the cipher text can gain information from the repeated blocks.
  - Some can even alter or rearrange the cipher text to his advantage.
- ECB is rarely used to encrypt messages.

Previous Next

CBC Mode of Encryption



CBC Mode of Decryption



- The receiver and sender must know key, and IV.
  - Or key, and the method to compute IV.

Previous Next

Threats on CBC Operation

- Modification of cipher text blocks.
- Changing c_i has predictable effect on P_{i+1} .
  - However, it also changes piin an unpredictable manner
- If the receiver is known to ignore pithen such attack is possible.
  - Possible safeguard is to attach a checksum (such as CRC) to the message before encryption.

PKI

- PKI Operations:
- Encryption, Decryption of short messages
- Digital signatures
- Authentication
- RSA: Uses modular exponents to make it computationally infeasible to recover message without key.
- Provided the message is carefully crafted. Keys are carefully selected.

Security Mechanism

- Confidentiality
  - Will an attacker make any sense out of a picked packet?
- Integrity
  - Is the message unaltered?
- Owner Integrity
  - Is the message really from that person?
- Authentication
  - Is it you?

Previous Next

Security Mechanism: Confidentiality

- Use of symmetric cipher.
- Encryption and decryption operations are needed.
- A Shared key is needed
    - Can be sent using PKI or any other reliable channel.

Security Mechanism: Integrity

- Map the message to smaller number of bits
    - Using one-way functions.
        - Message digest functions (such as MD5, SHA etc.)
        - Can be cryptographic functions as well.
- Send the mapped information on an alternate channel.
    - Confidentiality may be used.
- Or, send it along with the message
    - Confidentiality is a must.
- Integrity keys are different than the confidentiality keys.
    - Symmetric ciphers are used.

Previous Next

Authentication: Symmetric Cipher Based

- Challenge response
    - Challenger sends a random number to the subject.
- Subject gives a response to the challenge
    - Response derived using cryptography. For example, the encryption of the challenge using a shared key.

Owner Integrity: PKI

- Digital Signature
    - Can only be generated using the private key.
    - Can be verified using the public key.
- Since private key is one person,
    - Only the owner can generate it.
    - A document may be hashed and the hash may be signed digitally by the owner of the private key.
- Any one can verify the sign. Must have access to the public key of the signer.

Authentication: PKI

- Challenge-Response
    - Challenger can ask the subject to sign a random number
    - Challenger has access to the “certified” public key of the subject.
- Only subject can sign it correctly since it must have the access to the private key.
- Challenger can verify using public key.

Previous Next