Computer and Network Security

Lecture 4

Modern Block Ciphers

Administrative

- Slides have been published!
  - http://lsd.ls.fi.upm.es/lsd/education
- Contact
  - csoriente@fi.upm.es

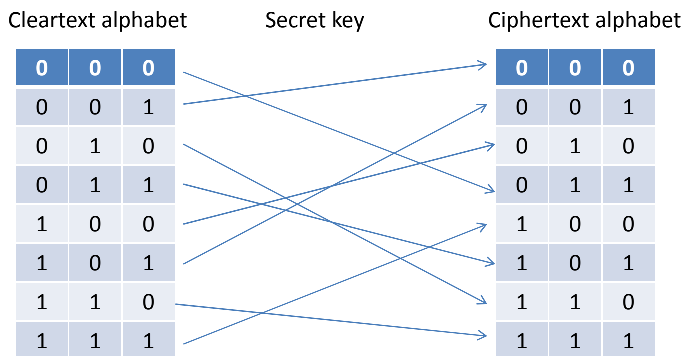
Outline

- Block-ciphers
  – Feistel Network
- DES
  – Attacks
  – Variants
- AES
  – History and mode of operation

Block Ciphers

- Encrypt/Decrypt data in blocks of N bits
  – E.g., N=64 or N=128
- See each block as a character
  – Alphabet of size 2^N
- Convert a block of plaintext to a block of ciphertext
  – $2^N!$ such mappings
- A secret key indicates which mapping to use

Example – N = 3



- Secret key = map cleartext ↔ ciphertext
- In general, with P alphabet symbols there are P! mappings
  – 2^3 = 9 symbols → 2^3! = 9! = 362 880 mappings

Ideal Block Cipher

- Use any of the 2^N! mappings
  – The key space would be extremely large
- But this would require a key of $\log_2(2^N!)$ bits
- If N = 64
  – $\log_2(2^N!) \approx 10^{11}$ GB
- Infeasible!

Practical Block Ciphers

- Modern block ciphers use a key of K bits to specify a random subset of 2^K mappings.
- If the selection of the 2^K mappings is **random**, the resulting cipher will be a good approximation of the **ideal** block cipher.
- Shannon's Confusion and difusion principle
  - A cipher should hide local parts in a language from the attacker
  - A cipher should mix around the diferent parts of the plaintext so that nothing is left in its original place.
- Horst Feistel's Cipher Structure (1973)

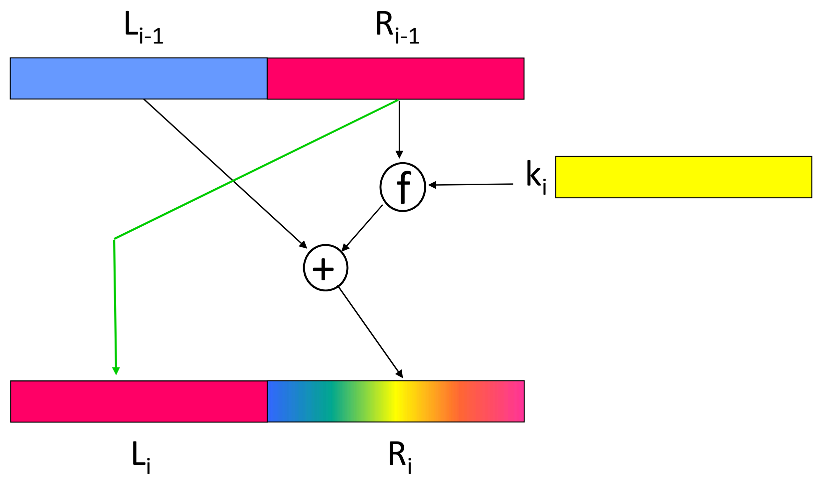
7

The Feistel Network

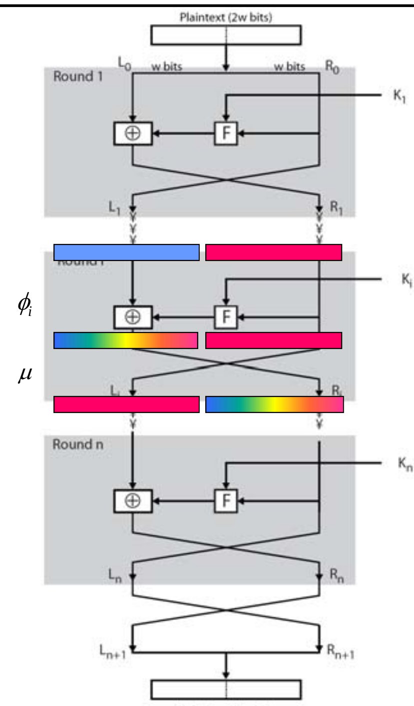
- Input
  - data block + key
- Algorithm
  - Repeat for r rounds
    - Compute a round key
    - Partition data block in two halves L and R
    - R does not change
    - L goes through an operation that depends on R and the round key
    - Swap L and R

8

i-th round



The Feistel Cipher Structure



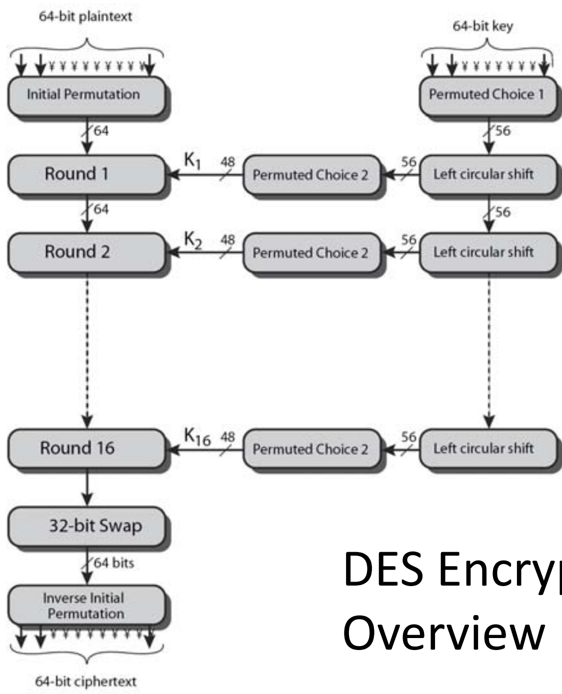
Fiestel Cipher Structure – Specs

- Block size
  - larger block sizes mean greater security
- Key Size
  - larger key size means greater security
- Number of rounds
  - multiple rounds offer increasing security
- Round key generation algorithm
  - greater complexity will lead to greater difficulty of cryptanalysis

DES: The Data Encryption Standard

- Most widely used block cipher in the world
- Adopted by NIST in 1977
- Based on the Feistel cipher structure with 16 rounds of processing
- Block = 64 bits
- Key = 56 bits
- Specific to DES
  - Design of the f() function
  - Round keys derivation

12



DES Encryption Overview

Attacks on DES

- Brute-force key search
  - Needs only two plaintext-ciphertext samples
  - O(2^{55})
- Differential cryptanalysis
  - Look for correlation between I/O
  - Possible to find a key with 2^{47} plaintext-ciphertext samples
  - Known-plaintext attack
- Liner cryptanalysis:
  - Look for correlations in bits of plaintext and ciphertext
  - Possible to find a key with 2^{43} plaintext-ciphertext samples
  - Known-plaintext attack

14

DES Cracker

- DES Cracker (1998)
  - A DES key search machine
  - contains 1536 chips
  - Cost: $250,000
  - could search 88 billion keys per second
  - won RSA Laboratory's "**DES Challenge II-2**"
    - 56 hours to find a key
- DES is feeling its age… a more secure cipher is needed

15

Multiple Encryption with DES

- In 2001, NIST published the Advanced Encryption Standard (AES) to replace DES
- But users in commerce and finance are not ready to give up on DES
- Temporary solution
  - Encrypt multiple times using multiple keys
    - 2DES
    - 3DES

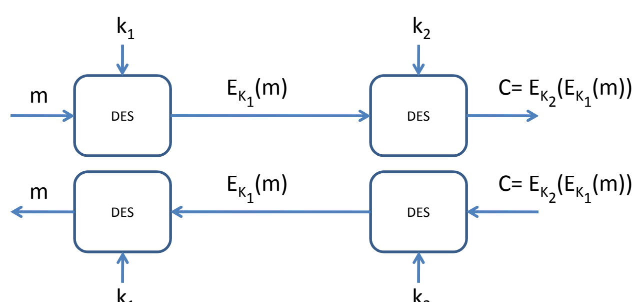
16

2DES

- Encryption
  - $c = E_{k_2}(E_{K_1}(m))$
- Decryption
  - $m = D_{k_1}(D_{k_2}(c))$
- Key length: 56 x 2 = 112 bits
- Does it mean $O(2^{111})$ steps to brute-force?
  - Not really!

17

Meet-in-the-Middle Attack on 2DES



- Given tow pairs (m, c) and (m', c')
  - Encrypt m with all 2^{56} possible keys for k_1
  - Decrypt c with all 2^{56} possible keys for k_2
  - If $E_{k_1'}(m) = D_{k_2'}(c)$, try these keys on (m', c')
  - If works, (K1', K2') = (K1, K2) with high probability.
  - Takes $O(2^{56})$ steps
    - Attacking DES takes $O(2^{55})$ steps

18

3DES with two keys

- Encryption
  - $c = E_{k_1}(E_{k_2}(E_{K_1}(m)))$
- In practice
  - $c = E_{k_1}(D_{k_2}(E_{K_1}(m)))$
- Also called EDE (Encryption-Decryption-Encryption)
- Backward compatibility
  - If $k_1=k_2$ → 3DES = DES
- No practical attacks up to date
- Standard ANSI X9.17 and ISO 8732

19

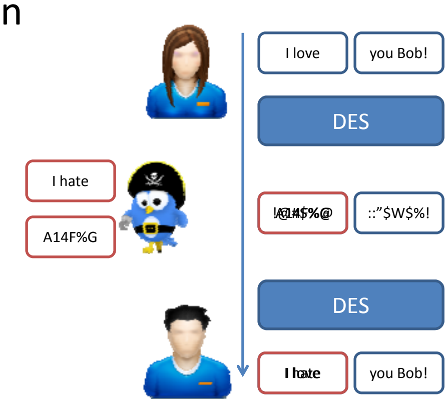
3DES with three keys

- Encryption
  - $c = E_{k_3}(E_{k_2}(E_{K_1}(m)))$
- Backward compatibility
  - If $k_1=k_3$ → 3DES w/ 3 keys = 3DES w/ 2 keys
  - If $k_1=k_2=k_3$ → 3DES w/ 3 keys = DES
- Used by some apps
  - E.g., PGP, S/MIME

20

Problems with block ciphers

- What if m is larger than a block size?
- Permutation / Substitution attack is trivial
- Several “mode” of operation



DES modes

- Block modes
  - Electronic code-book (ECB) $m_i = E_k(p_i)$
    - Local Error, parallel enc/dec
    - Same cleartext = Same ciphertext, perm/sub attack
  - Chained block cipher (CBC) $c_i = E_k(c_{i-1} \text{ XOR } m_i)$
    - Need IV, transmission error affects two blocks
- Stream modes
  - Output feedback (OFB) $v_i = E_k(v_{i-1})$ $c_i = m_i \text{ XOR } v_i$
    - Local error, pre-computation
  - Cipher feedback (CFB) $c_i = m_i \text{ XOR } E_k(C_{i-1})$
    - Error propagation

Advanced Encryption Standard

- National Institute of Science and Technology (NIST) regulates standardization in the US
- DES is an aging standard that no longer addresses today's needs for strong encryption
- Triple-DES: Endorsed by NIST as a "de facto" standard
- AES: Advanced Encryption Standard
  - Finalized in 2001
  - Goal is to define the Federal Information Processing Standard (FIPS) by selecting a new encryption algorithm suitable for encrypting government documents
  - Candidate algorithms must be:
    - Symmetric-key ciphers supporting 128, 192, and 256 bit keys
    - Royalty-Free
    - Unclassified (i.e. public domain)
    - Available for worldwide export

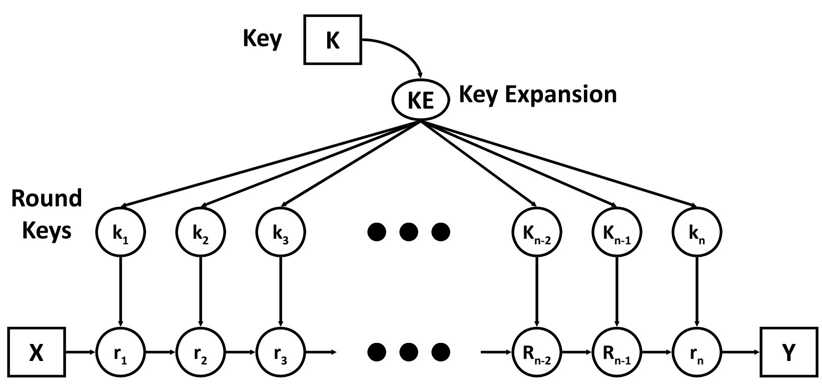
History

- AES Round-3 Finalist Algorithms:
  - MARS
    - Candidate offering from IBM
  - RC6
    - By Ron Rivest of MIT & RSA Labs, creator of the widely used RC4/RC5 algorithm and "R" in RSA
  - Twofish
    - From Counterpane Internet Security, Inc.
  - Serpent
    - by Ross Anderson, Eli Biham and Lars Knudsen
  - Rijndael
    - by Joan Daemen and Vincent Rijmen (KUL, Belgium)

The winner: Rijndael

- Joan Daemen and Vincent Rijmen
  - Proton World International
  - Katholieke Universiteit Leuven
- Key length
  - 128, 192, and 256
- Block length
  - 128, 192, and 256
    - AES only allows 128 bits
- Speed improvement over DES in both hw and sw implementations
  - 8.8 Mbytes/sec on a 200MHz Pentium Pro

Rijndael



Encryption Rounds $r_1 \ldots r_n$

- Key is expanded to a set of n round keys
- Input block X undergoes n rounds of operations (each operation is based on value of the n-th round key), until it reaches a final round.
- Strength of algorithm relies on the fact that it's very difficult to obtain intermediate result (or state) of round n from round n+1 without the round key.

Rijndael

- Secure
  - Immune to
    - Linear and differential cryptanalysis
    - Known-key and related-key attacks
    - Square attack
    - Interpolation attacks
    - Weak-keys
  - No key-recovery attacks faster than exhaustive search
- Future:
  - Rijndael is an extremely fast, state-of-the-art, highly secure algorithm
  - Amenable to efficient implementation in both hw and sw
  - Requires no special instructions to obtain good performance on any computing platform
  - However, Triple-DES, still highly secure and supported by NIST, is expected to be common for the foreseeable future