

Computing Topics lecture:

Block Ciphers

Michael Huth



Acknowledgements

- ▶ The slides of my lecture are based on the book
Cryptography Engineering: Design Principles and Practical Applications by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno (Wiley 2010)



Aims of my lecture on block ciphers

Make sure you understand

- ▶ what block ciphers are
- ▶ why their security is hard to define and achieve
- ▶ what modes for block ciphers are



Outline of lecture

Context of Cryptography

Block Ciphers

Modes of Operation



Context of Cryptography



Role of cryptography

- ▶ means for distinguishing and regulating “good” access from “bad” access to information
- ▶ but strong cryptography won't guarantee system security
- ▶ e.g. buffer-overflow attack on web application may circumvent need of attacking cryptography of system
- ▶ but broken cryptography may prevent detection of attack!

Therefore, it is important to get cryptography right in a system



Block Ciphers



Definition of block cipher

A block cipher is an encryption device for blocks of data of **fixed** size. One mathematical model of a block cipher is

- ▶ **key space** $\mathcal{K} \subseteq 2^m$ where m is bit-length of keys, typically 128 or 256
- ▶ bit-length l of blocks, typically 128 or 256
- ▶ two functions E and D of type $\mathcal{K} \times 2^l \rightarrow 2^l$
- ▶ $E(K, p)$ encryption of **plaintext** p with key K
- ▶ $D(K, c)$ decryption of **ciphertext** c with key K
- ▶ decrypting with same key recovers plaintext p :

$$D(K, E(K, p)) = p$$



Ideal Block Cipher

- ▶ $E(K, \cdot): 2^l \rightarrow 2^l$ random permutation for each K
- ▶ different permutations for different keys chosen independently, (no related-key attacks, etc.)
- ▶ that is, each K gives us random look-up table of 2^l many l bit words, and each table chosen at random.



Security of Block Cipher

- ▶ definition of attack: **non-generic** method of distinguishing given block cipher from ideal one
- ▶ open problem: how to define what generic means
- ▶ but attack definition subsumes known attack types
- ▶ similar problem: to define obscenity, we know it when we see it, but we cannot define it
- ▶ now we look at distinguishing method as an attack game



Attack games

- ▶ given ideal block cipher I and actual block cipher X
- ▶ attacker has access to black box B , which either implements I or X
- ▶ B either in encryption or decryption state, attacker can change state
- ▶ attacker can repeatedly input different plaintexts (or ciphertext) and keys
- ▶ attacker wins game if she has $> 1/2$ probability of predicting which of I and X box B implements



A generic attack

- ▶ attacker knows value of $E_X(0^m, 0^l)$ since cipher X is publicly known (**Kerckhoffs's Principle**)
- ▶ attacker feeds 0^m and 0^l into box B and compares its output with $E_X(0^m, 0^l)$
- ▶ this will distinguish I from X with probability $> 1/2$ since $E_I(0^m, \cdot): 2^l \rightarrow 2^l$ random permutation
- ▶ this attack is generic: does not exploit properties of X ; works for all choices of X
- ▶ more sophisticated but still generic attacks can be built

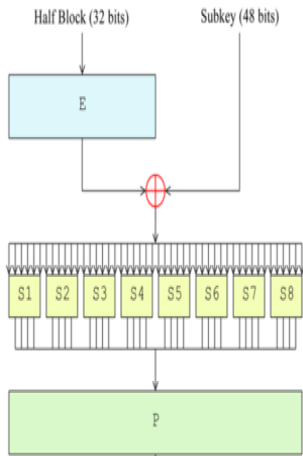


A real block cipher: DES

- ▶ operates in rounds
- ▶ block size is 64, key size is 56
- ▶ each round computes with Feistel function F
- ▶ each round schedules key determined by encryption key and round number
- ▶ Feistel function contains linear and non-linear components
- ▶ non-linear components (the S-boxes) only source of security



DES Feistel function F

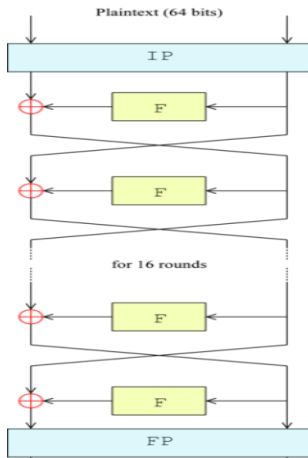


Fixed E inflates 32 bits to 48
key and round number yield 48-bit subkey
Eight fixed S -boxes reduce 6 bits to 4
Fixed permutation P produces output of F

Acknowledgment: [Wikipedia picture](#)



DES Feistel architecture



Initial, fixed permutation IP on plaintext
16 rounds on Feistel function F
round i uses key K_i derived from K
plaintext P equals L_0R_0

$$L_j = R_{j-1}$$

$$R_j = L_{j-1} \oplus F(R_{j-1}, K_j)$$

Output is result of fixed, final permutation

Acknowledgment: [Wikipedia picture](#)

Key size

- ▶ 56 bits for keys is insecure these days
- ▶ length of keys may have to be secure for 20+ years, without knowing how technology and mathematics will evolve
- ▶ recommended $2n$ bits for n bits of security, e.g. 256 bit keys at present
- ▶ designs require proportionality between key and block size
- ▶ blocks and keys cannot be too long, e.g. to minimize power consumption



Modes of Operation



Why block ciphers run in modes

- ▶ plaintext may be larger than one block
- ▶ need to divide plaintext into blocks
- ▶ triggers two issues
- ▶ first, how to pad the last block if it is shorter than l bits?
- ▶ second, how to use the block cipher on the blocks of the plaintext (**its mode**)
- ▶ we only look at the second question



Electronic Code Book Mode (ECB)

- ▶ plaintext p equals sequence of blocks $p_1 p_2 \dots p_k$
- ▶ modes generally produce ciphertext of blocks $c_1 c_2 \dots c_k$
- ▶ ECB computes $c_i = E(K, p_i)$
- ▶ each block encrypted in isolation with same key
- ▶ problematic: repeated encryption of plaintext yields same ciphertext



Cipher Block Chaining Mode (CBC)

- ▶ CBC computes $c_i = E(K, p_i \oplus c_{i-1})$
- ▶ ciphertext of previous block is XOR-ed with current plaintext before encryption
- ▶ but what to choose as c_0 ?
- ▶ this c_0 is known as **initialization vector** IV
- ▶ computation and handling of IV requires care



Decryption in CBC

- ▶ recall CBC encryption $c_i = E(K, p_i \oplus c_{i-1})$ where c_0 is *IV*
- ▶ decryption is $D(K, c_i) \oplus c_{i-1}$ since

$$\begin{aligned} D(K, c_i) \oplus c_{i-1} &= D(K, E(K, p_i \oplus c_{i-1})) \oplus c_{i-1} \\ &= p_i \oplus c_{i-1} \oplus c_{i-1} \\ &= p_i \end{aligned}$$

- ▶ but this requires decrypting party to know the *IV*



Illustrating problem with using ECB mode



Acknowledgment: [Wikipedia](#)



Conclusion

We discussed

- ▶ what block ciphers are
- ▶ why their security is hard to define and achieve
- ▶ what modes for block ciphers are
- ▶ why different applications may require different modes



Thank You for Your Kind Attention

Questions?

