CSC3631 Cryptography

Block Cipher

Changyu Dong

Newcastle University

Difference Between Block Ciphers and Stream Ciphers

- Stream ciphers encrypt bit-by-bit
- Block ciphers encrypt block-by-block
- Stream ciphers encrypt by substitution
  - Each bit in the plaintext is substituted by a random (pseudorandom) bit
- Block ciphers encrypt by substitution and transposition
  - The bits in a block also change positions

Similarities Between Block Ciphers and Stream Ciphers

- They all have an encryption function, an decryption function and security relies on a key.
- Abstractly, we can use the following to represent a blackbox symmetric key cipher
  - A pair of functions (E, D), a key k
  - To encrypt a message m into the corresponding ciphertext c, $c = E_k(m)$
  - To decrypt the ciphertext, $m = D_k(c)$
  - $D_k(E_k(m)) = m$

Block ciphers as pseudorandom permutations

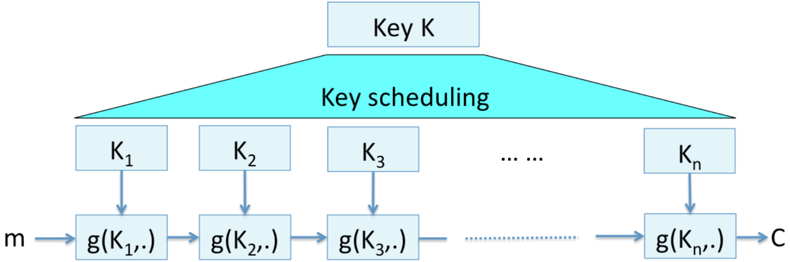
- A block cipher encrypts block by block.
- If the block is L-bit long, then there are 2^L possible bit patterns for the plaintext, and 2^L for the ciphertext.
- The plaintext is one-to-one mapped to the cihpertext (otherwise some ciphertext may not be decrypted correctly)
- Hence a permutation
- The mapping from plaintext to the cihpertext is unpredictable without the key
- Hence pseudorandom.

Design Criteria of Block Cipers

- Confusion: make the relationship between the key and resulting ciphertext as complex as possible
  - Each ciphertext value should depend upon several parts of the key
  - But this mapping between the key values and the ciphertext values seems to be completely random to the observer.
  - So the key cannot be uncovered from the ciphertext.
- Diffusion: a single plaintext bit or key has influence over all of the ciphertext bits.
  - Doesn't mean every bit will be changed
  - For a strong cipher, flipping 1 bit of the key or the plaintext is expected to flip about 50% of bits of the ciphertext
- Avalanche effect: A small change in the input must produce a very large difference in the output
  - Ideal, each bit in the output will be flipped with a probability of 0.5

Iterated construction

- Multiple rounds, each round uses the same round function a different sub-key.
  - The round function becomes small and easier to design
  - The round function is not entirely secure, but after composing them together, the cipher is secure – behave as a pseudorandom permutation.

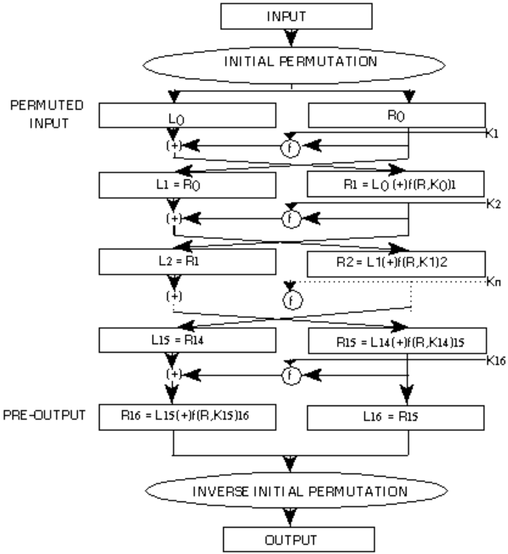


DES

- First standard cipher (US national standard from1977 to 2001)
- Block size 64 bits
- Key size 56 bits (plus 8 parity bits)
- 16 rounds
- Considered weak today mainly because its key space is too small now.

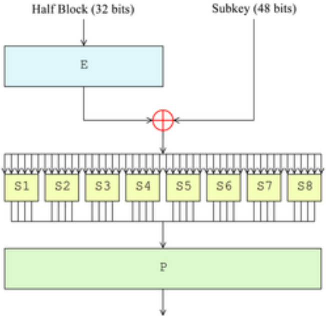
DES Internal

- An example of Feistel network
- Initial permutation (IP) changes the order of the bits in the plaintext
- 16-round
- Final permutation (FP) which is the inverse of IP
- IP and FP are public and don't have any effect on security
- Security depends on the f-function
- Decryption algorithm is the same, just use the keys in a reversed order



F-function

- E-box: expand 32-bit block into 48-bit using a fixed mapping
- S-box: 8 different s-boxes, each maps 6-bit into 4-bit. 48-bit $\rightarrow$ 32-bit
- P-box: rearranged bits from all s-boxes according to a fixed permutation



3-DES

- 56-bit key is weak
- But DES is widely implemented and used
- How to increase security without a completely new cipher?
- Apply DES to the same data multiple time with multiple keys.
- Security of 3-DES is equivalent to a 112-bit key cipher
- Several modes: EEE3, EDE3,EEE2,EDE2

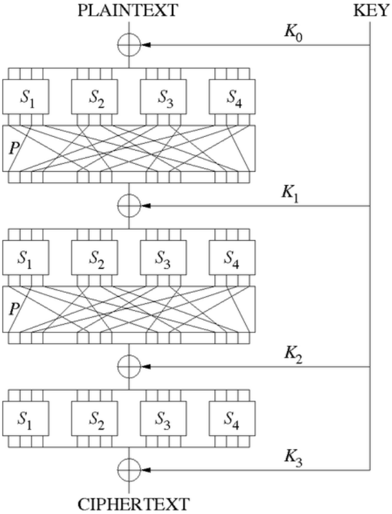
The Insecurity of 2-DES

- We have seen 3-DES, but not 2-DES
- This is because 2-DES doesn't increase security very much.
- We want the security to increase exponentially in the length of the key
  - 2-DES with 2*56 =112 bits
- However, the strength of 2-DES is only $2 * 2^{56} = 2^{56+1}$.
- Meet in the middle attack:
  - You have a plaintext and the corresponding ciphertext: $c = E_{k_2}(E_{k_1}(m))$
  - You try all possible keys to encrypt m and record the result $E_{k_i'}(m)$
  - You try all possible keys to decrypt c and record the result $D_{k_i''}(c)$
  - If you find a result is the same from the encryption and decryption, you know k_2 and k_1
  - Maximal $2 * 2^{56}$ operations and storage

Substitution-permutation network

- Another popular design paradigm of modern symmetric key block ciphers
- Consists of several rounds.
- Each round, bits go through substitution boxes (S-boxes) and permutation boxes (P-boxes)
  - S-box: substitutes a small block of bits (the input of the S-box) by another block of bits
  - P-box: a permutation of all the bits of all the S-boxes of one round, permutes the bits, and feeds them into the S-boxes of the next round.
- Each round, a round key is derived from the key is used
- Kind of similar to Feistel network, but
  - SPN has more parallelism – faster
  - FN doesn't require the S-boxes to be invertible, but SPN does.

Substitution-permutation network



AES

- New standard after DES
- Based on substitution-permutation network.
- The result of a 3 year worldwide review process.
- 128-bit block
- Key size (number of rounds):128 (10), 192 (12), 256 (14)
- Number of rounds is critical: known attacks on reduced rounds.
- All known attacks on full-AES are theoretical
- Fast due to many operations can be performed in parallel

Modes of Operation

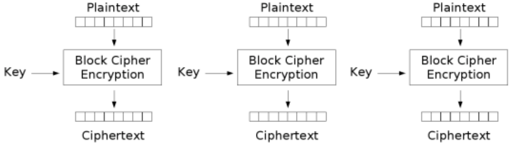
- Most time the plaintext you encrypt is larger than just 1 block
- Needs a way to encrypt an arbitrarily long plaintext

Padding

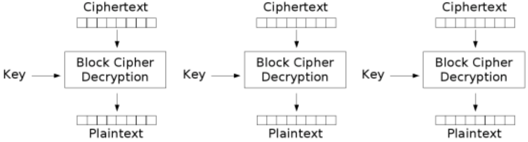
- Block ciphers require plaintext size to be a multiple of the block size
- If not, plaintext needs to be "padded".
- e.g. PKCS#7 padding: for $n > 0$, n byte pad is: $nnnn \dots n$
- Question: what if the plaintext is a multiple of block size?

Electronic Code Book Mode (ECB)

- Simplest mode
- Plaintext is broken into multiple blocks
- Each block is encrypted using the same key
- Decryption is the inverse



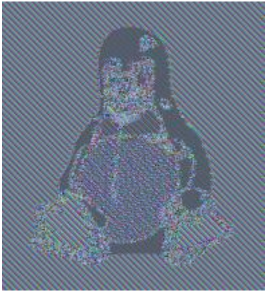
Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

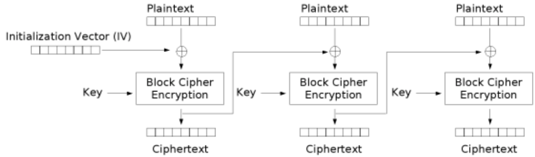
Problem of ECB

- Deterministic: Two identical plaintext blocks yield same ciphertext blocks
  - Can reveal pattern in the plaintext
  - Should be used only in encrypting small amount of data

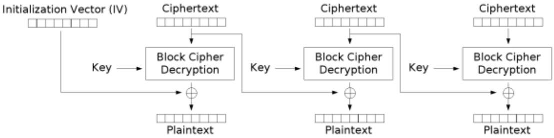


Cipher Block Chaining Mode (CBC)

- The first block in the plaintext is XORed with a random IV before encryption
- The subsequent blocks in the plaintex is XORed with the ciphertext of previous block before encryption



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Properties of CBC

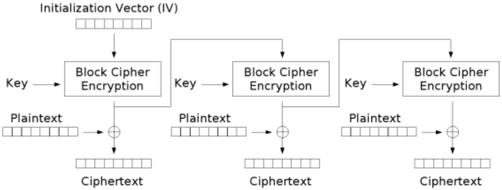
- Randomised encryption:repeated plaintext gets mapped to different encrypted ciphertext.
  - The randomness comes from the IV
  - If the IV is predicatble, then certain attacks are possible
  - IVs can be sent in clear
- A ciphertext block depends on all preceding plaintext blocks; reordering affects decryption

Output Feedback Mode (OFB)

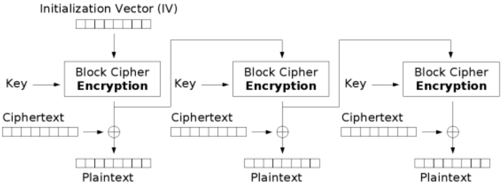
- In ECB and CBC modes, plaintext blocks pass through the encryption algorithm in some way
- In OFB, plaintext never goes through the encryption algorithm
- OFB uses the encryption algorithm to generate key stream
- It turns a block cipher into a stream cipher

Output Feedback Mode (OFB)

- An random IV is encrypted into the key stream for the first plaintext block
- The keystream is then encrypted into the key stream for the next plaintext block, and so on



Output Feedback (OFB) mode encryption



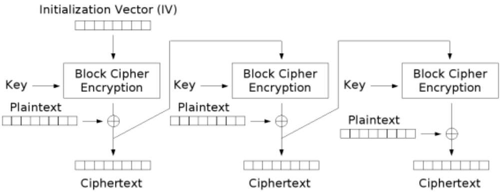
Output Feedback (OFB) mode decryption

Properties of OFB

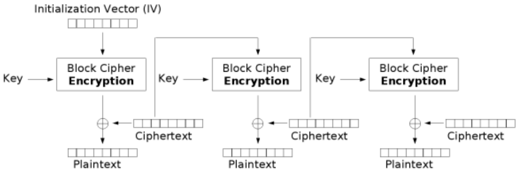
- As in CBC, requires random IV
- You don't need to implement the decryption algorithm of the block cipher
- Has all disadvantages of a stream cipher

Cipher Feedback Mode(CFB)

- Similar to OFB
- But now the ciphertext in each round is used as feedback



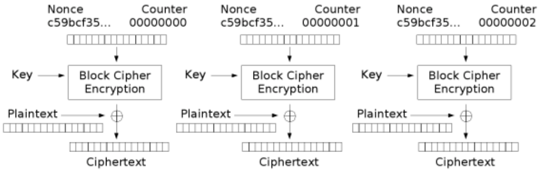
Cipher Feedback (CFB) mode encryption



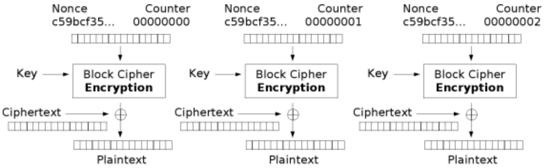
Cipher Feedback (CFB) mode decryption

Counter (CTR) mode

- Relatively new, not standardised until recently
- Also a stream cipher mode
- A key block is generated by encrypting the result of concatenating nonce with counter value



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Properties of CTR

- Keystream can be computed in parallel as multiple blocks
- Each block is encrypted independently
  - Encryption and decryption can be done in random order
  - Good for random access data

Reading

- Cryptography made simple §13.1 – 13.4
- Cryptography theory and practice §3.1, 3.2, 3.5 – 3.7
- Applied cryptography §12 – 14