

Block Ciphers

Gianluca Dini
Dept. of Ingegneria dell'Informazione

University of Pisa

gianluca.dini@unipi.it

Version: 2022-03-23

1

Block Ciphers

GENERAL CONCEPTS

Mar-22

Block Ciphers

2

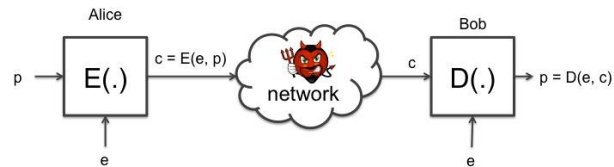
2

Block cipher



UNIVERSITÀ DI PISA

- Block ciphers break up the plaintext in blocks of fixed length n bits and encrypt one block at time



- $E_k: \{0,1\}^n \rightarrow \{0,1\}^n$ $D_k: \{0,1\}^n \rightarrow \{0,1\}^n$
- E is a keyed permutation: $E(k, m) = E_k(m)$
- $E_k(\cdot)$ is a permutation

Mar-22

Block Ciphers

3

3

Permutation



UNIVERSITÀ DI PISA

- E_k is a permutation
 - E_k is efficiently computable
 - E_k is bijective
 - Surjective (or onto)
 - Injective (or one-to-one)
 - E_k^{-1} is efficiently computable

Mar-22

Block Ciphers

4

4

True Random Cipher



UNIVERSITÀ DI PISA

- A True random cipher is perfect
- A true random cipher implements all possible Random permutations ($2^n!$)
 - Need a uniform random key for each permutation (naming)
 - key size $:= \log_2 (2n!) \approx (n - 1.44) 2^n$
 - Exponential in the block size!
 - The block size cannot be small in order to avoid a dictionary attack
- A true random cipher cannot be implemented

Mar-22

Block Ciphers

7

7

Pseudorandom permutations



UNIVERSITÀ DI PISA

- Consider a *family of permutations* parametrized by κ
 $\in K = \{0, 1\}^k$, $E_\kappa: \{0, 1\}^n \rightarrow \{0, 1\}^n$
- A E_κ is a *pseudorandom permutation* (PRP) if it is indistinguishable from a uniform random permutation by a limited adversary
- $|\{E_\kappa\}| = 2^k \ll |\text{Perm}_n|$, with $|\kappa| = k$
- A block cipher is a practical instantiation of a PRP

Mar-22

Block Ciphers

8

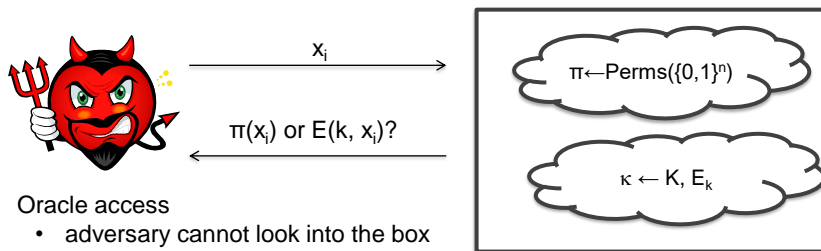
8

Practical block cipher



UNIVERSITÀ DI PISA

- In practice, the encryption function corresponding to a randomly chosen key should appear as a randomly chosen permutation to a limited adversary



- Oracle access
 - adversary cannot look into the box

Mar-22

Block Ciphers

9

9

Exhaustive key search



UNIVERSITÀ DI PISA

- The attack
 - Given a pair (pt, ct) , check whether $ct == E_{k_i}(pt)$, $i = 0, 1, \dots, 2^k - 1$
 - Known-plaintext attack
 - Time complexity: $O(2^k)$
- False positives
 - Do you expect that just one key k maps pt into ct ?
 - How many keys (false positives) do we expect to map pt into ct ?
 - How do you discriminate the good one?

Mar-22

Block Ciphers

10

10

Exhaustive key search



UNIVERSITÀ DI PISA

- False positives
 - Do you expect that just one key k maps pt into ct ?
 - How many keys (false positives) do we expect to map pt into ct ?
 - How do you discriminate the good one?

Mar-22

Block Ciphers

11

11

False positives



UNIVERSITÀ DI PISA

- Problem: Given (ct, pt) s.t. $ct = E_{k^*}(pt)$ for a given k^* , determine the number of keys that map pt into ct
- Solution.
 - Given a certain key k , $P(k) = \Pr[E_{k^*}(pt) == ct] = 1/2^n$
 - The *expected* number of keys that map pt into ct is $2^k \times 1/2^n = 2^{k-n}$

Mar-22

Block Ciphers

12

12

False positives



UNIVERSITÀ DI PISA

- Example 1 – DES with $n = 64$ and $k = 56$
 - On average 2^{-8} keys map pt into ct
 - One pair (pt, ct) is sufficient for an exhaustive key search
- Example 2 – Skipjack with $n = 64$ and $k = 80$
 - On average 2^{16} keys map pt into ct
 - Two or more plaintext-ciphertext pairs are necessary for an exhaustive key search

Mar-22

Block Ciphers

13

13

False positives



UNIVERSITÀ DI PISA

- Consider now t pairs (pt_i, ct_i) , $i = 1, 2, \dots, t$
 - Given k^* , $\Pr[E_{k^*}(pt_i) = ct_i, \text{ for all } i = 1, 2, \dots, t] = 1/2^{tn}$
 - Expected number of keys that map pt_i into ct_i , for all $i = 1, 2, \dots, t$, is $2^k/2^{tn} = 2^{k-tn}$
- Example 3 – Skypjack with $k = 80$, $n = 64$, $t = 2$
 - The expected number of keys is $= 2^{80 - 2 \times 64} = 2^{-48}$
 - Two pairs are sufficient for an exhaustive key search

Mar-22

Block Ciphers

14

14

False positives



UNIVERSITÀ DI PISA

- THEOREM
 - Given a block cipher with a key length of k bits and a block size of n bits, as well as t plaintext-ciphertext pairs, $(pt_1, ct_1), \dots, (pt_t, ct_t)$, the expected number of false keys which encrypt all plaintexts to the corresponding ciphertexts is 2^k
 - tn
- FACT
 - Two input-output pairs are generally enough for exhaustive key search

Mar-22

Block Ciphers

15

15

Block ciphers

EXERCISES

Mar-22

Block Ciphers

16

16

Exercise 1 - Exhaustive key search



UNIVERSITÀ DI PISA

- Exhaustive key search is a known-plaintext attack
- However, the adversary can mount a ciphertext-only attack if (s)he has some knowledge on PT

Mar-22

Block Ciphers

17

17

Exercise 1 – exhaustive key search



UNIVERSITÀ DI PISA

- Assume DES is used to encrypt 64-bit blocks of 8 ASCII chars, with one bit per char serving as parity bit
- How many CT blocks the adversary needs to remove false positives with a probability smaller than ϵ ?

Mar-22

Block Ciphers

18

18

Exercise 2 - dictionary attack



UNIVERSITÀ DI PISA

- Consider E with k and n .
- The adversary has collected D pairs (pt_i, ct_i) , $i = 1, \dots, D$, with $D \ll 2^n$
- Now the adversary reads C newly produced cyphertexts ct_j^* , $j = 1, \dots, C$.
- Determine the value of C s.t. the $\Pr[\text{Exists } j, j = 1, 2, \dots, C, \text{ s.t. } ct_j^* \text{ is in the dictionary}] = P$

Mar-22

Block Ciphers

19

19

Exercise 3 - Rekeying



UNIVERSITÀ DI PISA

- An adversary can successfully perform an exhaustive key search in a month.
- Our security policy requires that keys are changed every hour.
- What is the probability P that, in a month, the adversary is able to find any key before it is changed?
 - For simplicity assume that every month is composed of 30 days.
- What if we refresh key every minute?

Mar-22

Block Ciphers

20

20

Symmetric Encryption

MULTIPLE ENCRYPTION AND KEY WHITENING

Mar-22

Block Ciphers

21

21

Increasing the Security of Block Ciphers



UNIVERSITÀ DI PISA

- DES is a secure cipher
 - No efficient cryptanalysis is known
- DES key has become too short
- Can we improve the security of DES?
- Yes, by means of two techniques
 - Multiple encryption
 - Key whitening


Mar-22

Block Ciphers

22

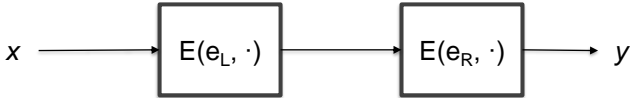
22

Two-times Encryption (2E)



UNIVERSITÀ DI PISA


- $y = 2E((e_L, e_R), m) = E(e_R, E(e_L, x))$
 - key size is $2k$ bits
 - Brute force attack requires 2^{2k} steps
 - 2E is two times slower than E
- Is it really secure?
- Meet-in-the-middle attack



Mar-22 Block Ciphers 23

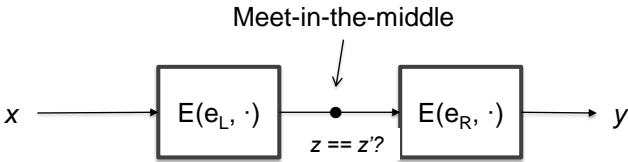
23

Meet-in-the-middle attack



UNIVERSITÀ DI PISA

- Attack Sketch
 1. Build a table T containing $z = E(e_L, x)$ for all possible keys e_L . Keep T sorted according to z .
 2. Check whether $z' = D(e_R, y)$ is contained in the table T , for all possible key e_R .
 1. If z' is contained in T then (e_L, e_R) maps x into y with e_L s.t. $T[e_L] = z'$.



Mar-22 Block Ciphers 24

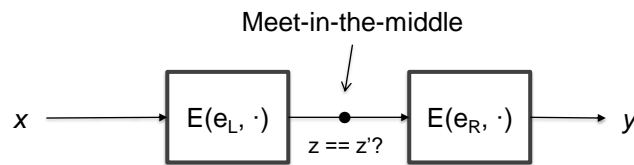
24

Meet-in-the-middle attack



UNIVERSITÀ DI PISA

- Attack complexity
 - Storage complexity
 - Storage necessary for table $T \approx O(2^k)$
 - Time complexity
 - Time complexity for step 1 + Time complexity for step 2 = Time for building and sorting the table + Time for searching in a sorted table = $k 2^k + k 2^k \approx O(2^k)$



Mar-22

Block Ciphers

25

25

Two-times DES



UNIVERSITÀ DI PISA

- 2DES
 - Time complexity: 2^{56} (doable nowadays!)
 - Space complexity: 2^{56} (lot of space!)
 - 2DES brings no advantage


Mar-22

Block Ciphers

26

26

Triple DES (3DES)



UNIVERSITÀ DI PISA

- EDE scheme
 - Standard ANSI X9.17 and ISO 8732
 - $Y = 3E((e_1, e_2, e_3), x) = E(e_1, D(e_2, E(e_3, x)))$
 - If $e_1 = e_2 = e_3$, 3DES becomes DES
 - backward compatibility
 - Key size = 168-bits
 - 3 times slower than DES
 - Simple attack $\approx 2^{118}$


Mar-22

Block Ciphers

27

27

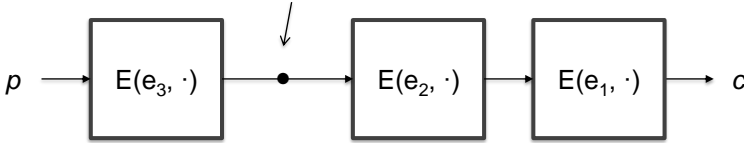
3DES – meet-in-the-middle attack



UNIVERSITÀ DI PISA

- Time = 2^{112} (undoable!)
- Space = 2^{56} (lot of space!)

Meet-in-the-middle



```
graph LR; p --> E3["E(e3, ·)"]; E3 --> dot(( )); dot --> E2["E(e2, ·)"]; E2 --> E1["E(e1, ·)"]; E1 --> c;
```

Mar-22

Block Ciphers

28

28

False positives for multiple encryption



UNIVERSITÀ DI PISA

- THEOREM

- Given there are r subsequent encryptions with a block cipher with a key length of k bits and a block size of n bits, as well as t plaintext-ciphertext pairs, $(pt_1, ct_1), \dots, (pt_t, ct_t)$, the expected number of false keys which encrypt all plaintext to the corresponding ciphertext is $2^{rk - tn}$

Mar-22

Block Ciphers

29

29

Limitations of 3DES



UNIVERSITÀ DI PISA

- 3DES resists brute force but
 - It is not efficient regarding software implementation
 - It has a short block size (64 bit)
 - A drawback if you want to make a hash function from 3DES, for example
 - Key lengths of 256+ are necessary to resist quantum computing attack

Mar-22

Block Ciphers

30

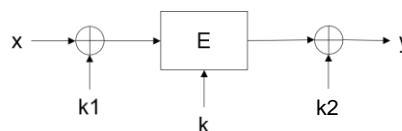
30

Key whitening



UNIVERSITÀ DI PISA

- Considerations
 - KW is not a “cure” for weak ciphers
- Applications
 - DESX: a variant of DES
 - AES: uses KW internally
- Performance
 - Negligible overhead w.r.t. E (Just two XOR's!)



Definition 5.3.1 Key whitening for block ciphers

Encryption: $y = e_{k,k_1,k_2}(x) = e_k(x \oplus k_1) \oplus k_2$

Decryption: $x = e_{k,k_1,k_2}^{-1}(y) = e_k^{-1}(y \oplus k_2) \oplus k_1$

Mar-22

Block Ciphers

31

31

Key whitening



UNIVERSITÀ DI PISA

- Attacks
 - Brute-force attack
 - Time complexity: 2^{k+2n} encryption ops
 - Meet-in-the-middle:
 - Time complexity 2^{k+n}
 - Storage complexity: 2^n data sets
 - The most efficient attack
 - If the adversary can collect 2^m pt-ct pairs, then time complexity becomes 2^{k+n-m}
 - The adversary cannot control m (rekeying)
 - Example: DES ($m = 32$)
 - Time complexity 2^{88} encryptions (nowadays, out of reach)
 - Storage complexity 2^{32} pairs = 64 GBytes of data (!!!)

Mar-22

Block Ciphers

32

32

Symmetric Encryption

ENCRYPTION MODES

Mar-22

Block Ciphers

33

33

Encryption Modes



UNIVERSITÀ DI PISA

- A block cipher encrypts PT in fixed-size n -bit blocks
- When the PT len exceeds n bits, there are several modes to use the block cipher
 - Electronic Codebook (ECB)
 - Cipher-block Chaining (CBC)


Mar-22

Block Ciphers

34

34

Other encryption modes



UNIVERSITÀ DI PISA

- Other encryption modes
 - To build a stream cipher out of a block cipher
 - Cipher Feedback mode (CFB)
 - Output Feedback mode (OFB)
 - Counter mode (CTR)
 - Authenticated encryption
 - Galois Counter mode (GCM, CCM, ...)
 - and many others (e.g., CTS, ...)
- Block ciphers are very versatile components


Mar-22

Block Ciphers

35

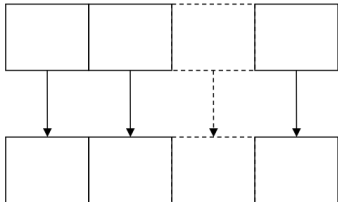
35

Electronic codebook

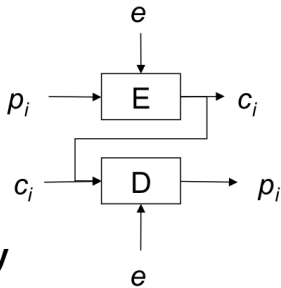


UNIVERSITÀ DI PISA

plaintext



ciphertext

$$\forall 1 \leq i \leq t, c_i \leftarrow E(e, p_i)$$
$$\forall 1 \leq i \leq t, p_i \leftarrow D(e, c_i)$$


PT blocks are encrypted separately

Mar-22

Block Ciphers

36

36

ECB - properties



UNIVERSITÀ DI PISA

- PROS
 - No block synchronization is required
 - No error propagation
 - One or more bits in a single CT block affects decryption of that block only
 - Can be parallelized
- CONS (it is insecure)
 - Identical PT results in identical CT
 - ECB doesn't hide data pattern
 - ECB allows traffic analysis
 - Blocks are encrypted separately
 - ECB allows block re-ordering and substitution

Mar-22

Block Ciphers

37

37

ECB doesn't hide data patterns



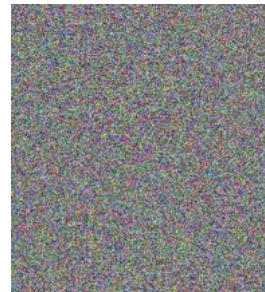
UNIVERSITÀ DI PISA



Plaintext



ECB encrypted



Non-ECB encrypted

Mar-22

Block Ciphers

38

38

ECB – block attack



UNIVERSITÀ DI PISA

- Bank transaction that transfers a customer C's amount of money D from bank B1 to bank B2
 - Bank B1 debits D to C
 - Bank B1 sends the "credit D to C" message to bank B2
 - Upon receiving the message, Bank B2 credits D to C
- Credit message format
 - Src bank: M (12 byte)
 - Rcv bank: R (12 byte)
 - Customer: C (48 byte)
 - Bank account number: N (16 byte)
 - Amount of money: D (8 byte)
- Cipher: $n = 64$ bit; ECB mode

Mar-22

Block Ciphers

39

39

ECB – block attack



UNIVERSITÀ DI PISA

- Mr. Lou Cipher is a client of the banks and wants to make a fraud
- Attack aim
 - To replay Bank B1's message "credit 100\$ to Lou Cipher" many times
- Attack strategy
 - Lou Cipher activates multiple transfers of 100\$ so that multiple messages "credit 100\$ to Lou Cipher" are sent from B1 to B2
 - The adversary identifies at least one of these messages
 - The adversary replies the message several times

Mar-22

Block Ciphers

40

40

ECB – block attack

- The fraud
 - Mr. Lou Cipher performs k equal transfers
 - credit 100\$ to Lou Cipher $\rightarrow c_1$
 - credit 100\$ to Lou Cipher $\rightarrow c_2$
 - ...
 - credit 100\$ to Lou Cipher $\rightarrow c_k$
 - Then, he searches for “his own” CTs, namely k equal CTs!
 - Finally he replies one of these cryptograms (many times)

Mar-22

Block Ciphers

41

41

ECB – block attack

- The message lacks any notion of time so it can be easily replied
- An 8-byte timestamp field T (block #1) is added to the message to prevent replay attacks
- A replied message can now be discarded

block no.	1	2	3	4	5	6	7	8	9	10	11	12	13
	T	M	R					C			N		D

Mar-22

Block Ciphers

42

42

ECB – block attack



UNIVERSITÀ DI PISA

- However, Mr Lou Cipher can still perform the attack
 1. Identify “his own” CTs by inspecting blocks #2-#13
 2. Select any his-own-CT
 3. Substitute block #1 of his-own-CT with block #1 of any intercepted “fresh” block
 4. Replay the resulting CT

Mar-22

Block Ciphers

43

43

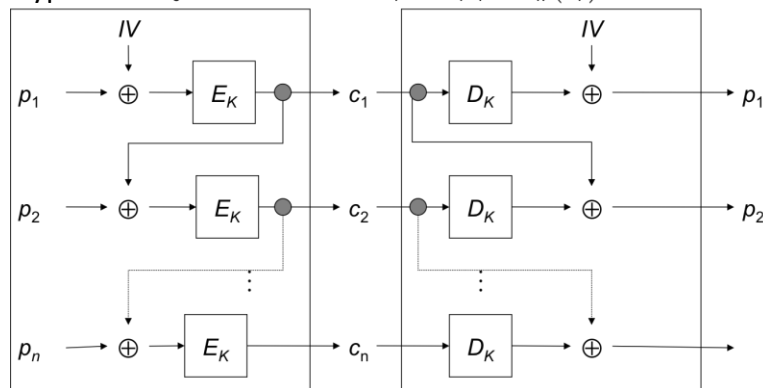
Cipher block chaining (CBC)



UNIVERSITÀ DI PISA

Encryption: $c_0 \leftarrow IV. \forall 1 \leq i \leq t, c_i \leftarrow E_K(p_i \oplus c_{i-1})$

Decryption: $c_0 \leftarrow IV. \forall 1 \leq i \leq t, p_i \leftarrow c_{i-1} \oplus D_K(c_i)$



Mar-22

Block Ciphers

44

44

CBC – properties (→)



UNIVERSITÀ DI PISA

- CBC mode is CPA-secure
- Chaining dependencies: c_i depends on p_i and the preceding PT blocks
- Cyphertext expansion is just one block
- CBC-Enc is *randomized* by using IV (nonce)
 - Identical ciphertext results from the same PT under the same key and IV
- CT-block reordering affects decryption

Mar-22

Block Ciphers

45

45

CBC – properties



UNIVERSITÀ DI PISA

- IV can be sent in the clear but its integrity must be guaranteed
- CBC suffers from Error propagation
 - Bit errors in c_i affect p_i and p_{i+1} (*error propagation*)
 - CBC is self-synchronizing (*error recovery*)
 - CBC does not tolerate “lost” bits (*framing errors*)
- CBC-dec can be parallelized

Mar-22

Block Ciphers

46

46

CBC – block attack



UNIVERSITÀ DI PISA

- If Bank A chooses a random IV for each wire transfer the attack will not work
- However, if Lou Cipher substitutes blocks #5 – #10 and #13, bank B would decrypt *account number* and *deposit amount* to random numbers => this is highly undesirable!
- Encryption itself is not sufficient, we need additional mechanisms (MDC, MAC, digsig) to protect integrity

Mar-22

Block Ciphers

47

47

Chosen-Plaintext Attack (Informal)



UNIVERSITÀ DI PISA

- CPA Attack
 - Attacker *makes* the sender to encrypt x_1, \dots, x_t
 - The attacker may influence or control encryption
 - The sender encrypts and transmits $y_1 = E_k(m_1), \dots, y_t = E_k(m_t)$
 - Later on, the sender encrypts x and transmits $y = E_k(m)$
- CPA-security guarantees that the adversary cannot learn anything about x
- The encryption scheme must be randomized

Mar-22

Block Ciphers

48

48

CPA model

The diagram illustrates the CPA model. On the left, a sender (blue person) sends a ciphertext $y = E_k(x)$ to a receiver (green person) on the right. Both are labeled with a key k . An attacker (red devil) is positioned below the sender, intercepting the ciphertexts y_1, y_2, \dots, y_t sent by the sender. The sender also sends a sequence of plaintexts x_1, x_2, \dots, x_t to the attacker. The attacker is shown with a magnifying glass over the ciphertext y . The University of Pisa logo is in the top right corner.

Mar-22

Block Ciphers

49

49

Block Ciphers

MORE ENCRYPTION MODES: OFB, CFB, CTR, CTS

Mar-22

Block Ciphers

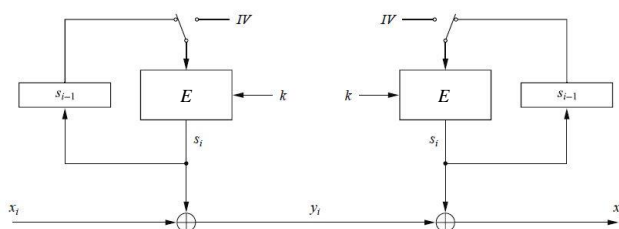
50

50

Output Feedback Mode (OFB)



UNIVERSITÀ DI PISA



Let $e()$ be a block cipher of block size b ; let x_i , y_i and s_i be bit strings of length b ; and IV be a nonce of length b .

Encryption (first block): $s_1 = e_k(IV)$ and $y_1 = s_1 \oplus x_1$

Encryption (general block): $s_i = e_k(s_{i-1})$ and $y_i = s_i \oplus x_i$, $i \geq 2$

Decryption (first block): $s_1 = e_k(IV)$ and $x_1 = s_1 \oplus y_1$

Decryption (general block): $s_i = e_k(s_{i-1})$ and $x_i = s_i \oplus y_i$, $i \geq 2$

Mar-22

Block Ciphers

51

51

Output Feedback Mode (OFB)



UNIVERSITÀ DI PISA

- OFB builds a stream cipher out of a block cipher
- The key stream is generated block-wise
- OFB is a *synchronous* stream cipher
- The receiver does not use decryption
- IV should be a nonce and make OFB non-deterministic
- Since OFB is synchronous, pre-computation of key stream blocks is possible

Mar-22

Block Ciphers

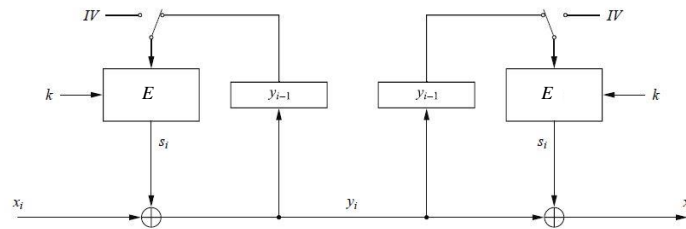
52

52

Cipher Feedback Mode (CFB)



UNIVERSITÀ DI PISA



Definition 5.1.4 Cipher feedback mode (CFB)

Let $e()$ be a block cipher of block size b ; let x_i and y_i be bit strings of length b ; and IV be a nonce of length b .

Encryption (first block): $y_1 = e_k(IV) \oplus x_1$

Encryption (general block): $y_i = e_k(y_{i-1}) \oplus x_i, \quad i \geq 2$

Decryption (first block): $x_1 = e_k(IV) \oplus y_1$

Decryption (general block): $x_i = e_k(y_{i-1}) \oplus y_i, \quad i \geq 2$

Mar-22

Block Ciphers

53

53

Cipher Feedback Mode (CFB)



UNIVERSITÀ DI PISA

- OFB builds a stream cipher out of a block cipher
- CFB is an *asynchronous* stream cipher as the key stream is also a function of the CT
- Key stream is generated block-wise
- IV is a nonce and makes CFB nondeterministic

Mar-22

Block Ciphers

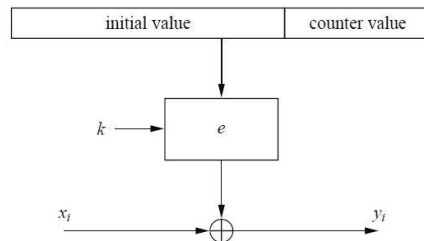
54

54

Counter Mode (CTR)



UNIVERSITÀ DI PISA



Definition 5.1.5 Counter mode (CTR)

Let $e()$ be a block cipher of block size b , and let x_i and y_i be bit strings of length b . The concatenation of the initialization value IV and the counter CTR_i is denoted by $(IV||CTR_i)$ and is a bit string of length b .

Encryption: $y_i = e_k(IV||CTR_i) \oplus x_i, \quad i \geq 1$

Decryption: $x_i = e_k(IV||CTR_i) \oplus y_i, \quad i \geq 1$

Mar-22

Block Ciphers

55

55

Counter Mode (CTR)



UNIVERSITÀ DI PISA

- CTR prevents two-time pad (keystream reuse)
- CTR can be parallelized
- Counter can be a regular counter or a more complex functions, e.g., LFSR
- Ciphertext expansion is just one block
 - Output y_0, y_1, \dots, y_t with $y_0 = (IV||ctr_0)$ being the the *expansion block*
 - $IV||ctr_0$ does not have to be kept secret
 - Can be transmitted together with $ct\ y_i$

Mar-22

Block Ciphers

56

56

CTR is CPA-secure



UNIVERSITÀ DI PISA

- A block cipher is a good approximation of a PRP (PRF), so the sequence $E_k(iv \parallel ctr_0+1), \dots, E_k(iv \parallel ctr_0+t)$ is pseudorandom
 - Two-time pad when $(iv \parallel ctr_0+i)$ wraps around → limit to the maximum number of messages you can encrypt
 - Two-time pad when $(iv \parallel ctr_0+i) = (iv' \parallel ctr_0' + j)$ but the probability of this event is exponentially small

Mar-22

Block Ciphers

57

57

Ciphertext Stealing (CTS) mode



UNIVERSITÀ DI PISA

- CTS allows encrypting PT that is not evenly divisible into blocks without resulting in any ciphertext expansion
- $\text{sizeof}(\text{ciphertext}) = \text{sizeof}(\text{plaintext})$
- CTS operates on the last two blocks
 - A portion of the 2nd-last CT block is stolen to pad the last PT block

Mar-22

Block Ciphers

58

58

Ciphertext stealing (CTS)

ECB mode

(from Wikipedia)

Diagram illustrating ECB mode encryption. Plaintext blocks P_{i-1} , P_i , and P_{i+1} are shown. P_{i-1} is encrypted to E_{i-1} . P_i is split into a 'Head' and 'Tail'. The 'Head' is encrypted to C_{i-1} , and the 'Tail' is encrypted to C_i . A dashed line labeled D_i connects the 'Tail' of P_i to the 'Head' of P_{i+1} .

CBC mode

(from Wikipedia)

Diagram illustrating CBC mode encryption. Plaintext blocks are XORed with the previous ciphertext block (or an initialization vector) and then encrypted using a key. The resulting ciphertext blocks are concatenated. The final ciphertext block is padded with zeros.

Look at [Wikipedia](https://tinyurl.com/dppr3b2m) for a detailed treatment (<https://tinyurl.com/dppr3b2m>)

Mar-22

Block Ciphers

59

Block Ciphers

PADDING

Mar-22


Block Ciphers

60

Foundations of Cybersecurity

30

The need for a padding scheme



UNIVERSITÀ DI PISA

Naïve (wrong) solution: Pad the message with zeroes to the right, without ambiguous boundaries

0x00

0x00

0x00

0x00

Problem: What if the message was a NULL-terminated string?

0x00

At the receiving side: Was it a NULL-terminated string or a 7-bytes pt?


Mar-22

Block Ciphers

61

61

The PKCS#5 padding scheme



UNIVERSITÀ DI PISA

- Padding is necessary when PT len is not an integer multiple of the block

If PT len is NOT a block multiple

- We need b padding bytes
- Fill each padding byte by b

Example: b = 3 then append 0x030303

Block

H

E

L

L

O

3

3

3

If PT is a block multiple

Padding = block

Fill each padding block by b

8

8

8

8

8

8

8

8

Padding causes *ciphertext expansion*

Mar-22

Block Ciphers

62

62

PKCS #5: encryption



UNIVERSITÀ DI PISA

- Let L be the block length (in bytes) of the cipher
- Let b be the # of blocks that need to be appended to the plaintext to get its length a multiple of L
 - $1 \leq b \leq L$
- Before encryption
 - Append b (encoded in 1 byte), b times
 - i.e., if $b = 3$, append $0x030303$

Mar-22

Block Ciphers

63

63

PKCS #5: decryption



UNIVERSITÀ DI PISA

- After decryption, say the final byte has value b
 - If $b = 0$ or $b > L$, return “error”
 - If the trailing b bytes are not all equal to b , return “error”
 - Strip off the trailing b bytes and output the left as the message

Mar-22

Block Ciphers

64

64

Block Ciphers

PADDING ORACLE ATTACK

Mar-22

Block Ciphers

65

65

Padding Oracle Attack



UNIVERSITÀ DI PISA

- The attacker
 - intercepts y and wants to obtain x
 - modifies y into y' and submits to the receiver
- The receiver (the padding oracle)
 - Returns “error”, if x' is not properly formatted
- On padding oracles
 - Frequently present in web applications
 - Error, receiver timing, receiver behaviour,...

Mar-22

Block Ciphers

66

66

Main idea of the attack

- For simplicity, let the ciphertext be a two-block ciphertext (IV, y) , with $y = E_k(x)$
 - So, at the receiving site, $x = D_k(y) \oplus IV$
- Message x is well formatted (padding)
- Main intuition
 - If the attacker changes the i th byte of IV , this causes a predictable change (only) to the i th byte of x'

Mar-22

Block Ciphers

67

67

The attack – step 1 – padding lenght

$D_k(y)$

yy	yy	yy	yy	yy	yy	yy	yy
----	----	----	----	----	----	----	----

\oplus

IV

AB	01	4F	21	00	7C	02	9E
----	----	----	----	----	----	----	----

$=$

x

XX	XX	XX	XX	XX	XX	XX	XX
----	----	----	----	----	----	----	----

Mar-22

Block Ciphers


68

68

Foundations of Cybersecurity

34

The attack – step 1 – padding lenght


UNIVERSITÀ DI PISA

$D_k(y)$

yy	yy	yy	yy	yy	yy	yy	yy
----	----	----	----	----	----	----	----

\oplus

IV

AB	01	4F	21	00	7C	02	9E
----	----	----	----	----	----	----	----

$\leftarrow 9F = 9E \oplus 06 \oplus 07$

$=$

x

XX	XX	06	06	06	06	06	06
----	----	----	----	----	----	----	----

$\leftarrow 07$


Mar-22

Block Ciphers

69

69

The attack – step 1 – padding lenght


UNIVERSITÀ DI PISA

$D_k(y)$

yy	yy	yy	yy	yy	yy	yy	yy
----	----	----	----	----	----	----	----

\oplus

IV

AB	01	4E	20	01	7D	03	9F
----	----	----	----	----	----	----	----

$=$

x

XX	XX	07	07	07	07	07	07
----	----	----	----	----	----	----	----

Mar-22

Block Ciphers


70

70

Foundations of Cybersecurity

35

The attack – step 1 – padding lenght


UNIVERSITÀ DI PISA

$D_k(y)$

yy	yy	yy	yy	yy	yy	yy	yy
----	----	----	----	----	----	----	----

\oplus

IV

AB	41	4E	20	01	7D	03	9F
----	----	----	----	----	----	----	----

=

x

XX	07	07	07	07	07	07	07
----	----	----	----	----	----	----	----


Mar-22

Block Ciphers

71

71

Attack complexity


UNIVERSITÀ DI PISA

- At most L tries to learn the # of padding bytes
- At most $2^8 = 256$ tries to learn each plaintext byte

Mar-22

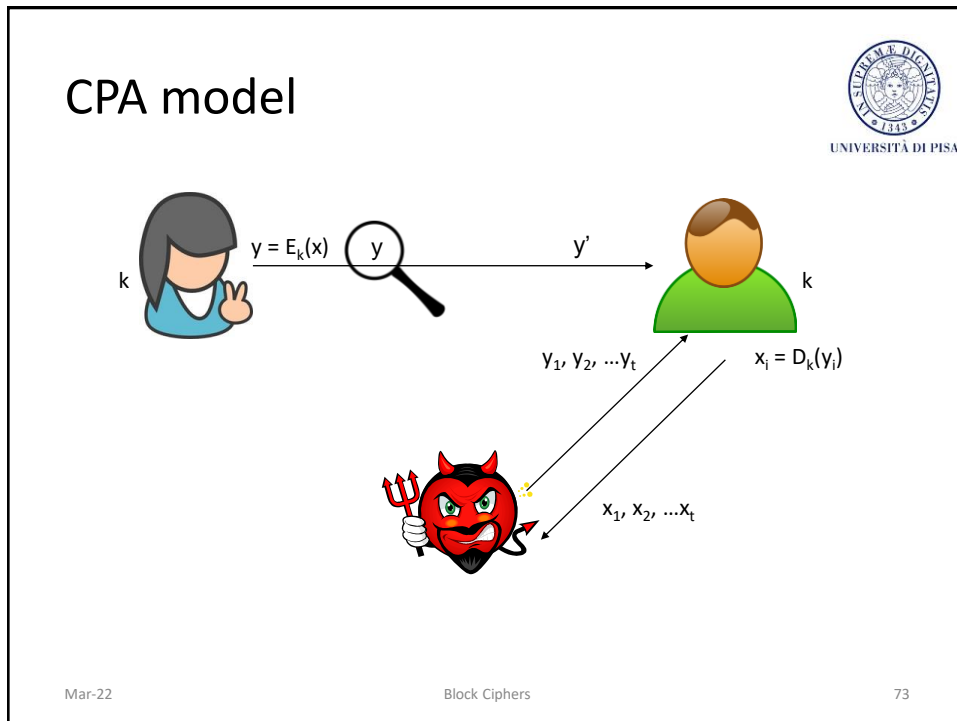
Block Ciphers

72

72

Foundations of Cybersecurity

36



73

Chosen-ciphertext attack

$y = E_k(x)$ y y' k $x_i = D_k(y_i)$ y_1, y_2, \dots, y_t x_1, x_2, \dots, x_t

- Now the attacker becomes active
- The CCA
 - The attacker intercepts $y = E_k(x)$ and modifies it into y'
 - The receiver decrypts y' and returns (the attacker) either x' or some information about x'
 - The adversary can derive either x or some information about x
- CCA and malleability
 - CCA-security implies non-malleability

Mar-22 Block Ciphers 74

74

CCA-security



UNIVERSITÀ DI PISA

- Chosen-ciphertext attacks represent a significant, real-world threat
- Modern encryption schemes are designed to be CCA-secure

Mar-22

Block Ciphers

75

75

Mar-22

Block Ciphers

76

76