Secret-Key Encryption

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Introduction to Cryptography

What is security?

C I A

Confidentiality

packet sniffing,
steal password

Integrity

packet spoofing
ARP cache poisoning
DNS " "
TCP session Hijacking.
Man-in-the-Middle.

Availability

Denial of Service attack,
SYN
TCP RST.

Crypto

Secret key Encryption (Symmetric key)
Public key Encryption (Asymmetric)
One-way Hash.

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Classical Cryptosystems

Classical Cryptosystems

Substitution Cipher (2000, Julius Caesar)

A → H

B → Z

⋮

Z → O

plaintext. Hello

P_1 P_2 P_3 P_4

Ciphertex. x t b b w

O → Z

th

Monoalpabetic Substitution Cipher.

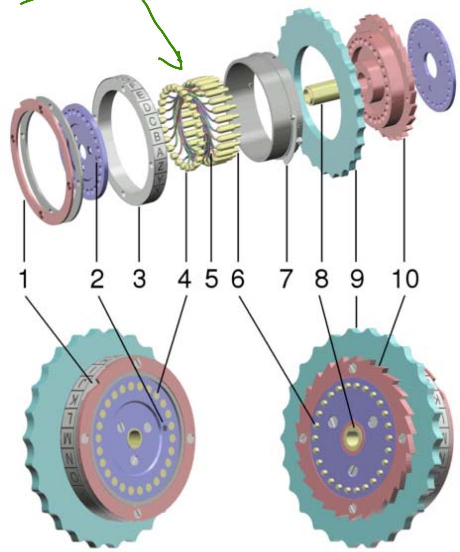
poly " " "

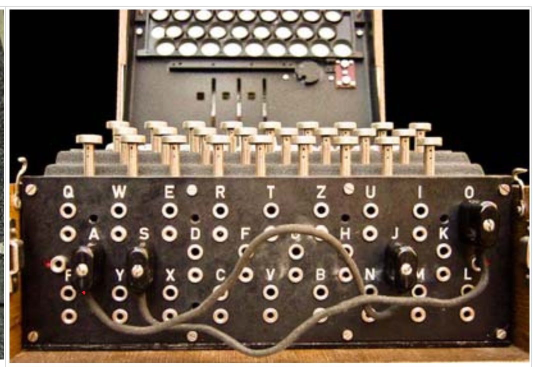
Enigma Machine

A → H

$26 \times 26 \times 26 \times 26$

permutation

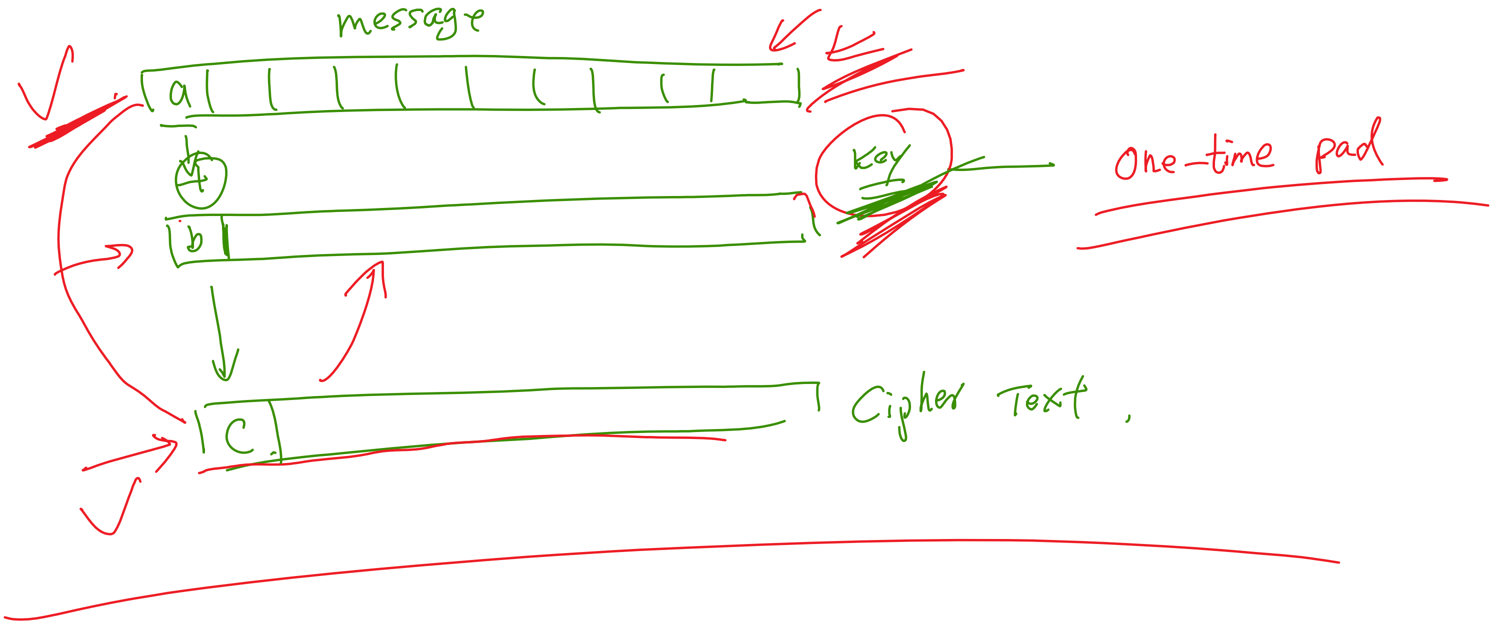




Combining the three rotors from sets of five, the rotor settings with 26 positions, and the plugboard with ten pairs of letters connected, the military Enigma has 158,962,555,217,826,360,000 (158 quintillion) different settings.[20]

Enigma was designed to be secure even if the rotor wiring was known to an opponent, although in practice there was considerable effort to keep the wiring secret. If the wiring is secret, the total number of possible configurations has been calculated to be around 10^{114} (approximately 380 bits); with known wiring and other operational constraints, this is reduced to around 10^{23} (76 bits).[9] Users of Enigma were confident of its security because of the large number of possibilities; it was not then feasible for an adversary to even begin to try every possible configuration in a brute force attack.

One-Time Pad



SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

DES:
Data Encryption Standard

DES: History

IBM: Horst Fiestel

"Lucifer"

1974. NIST

DES: 56 bits

NSA:

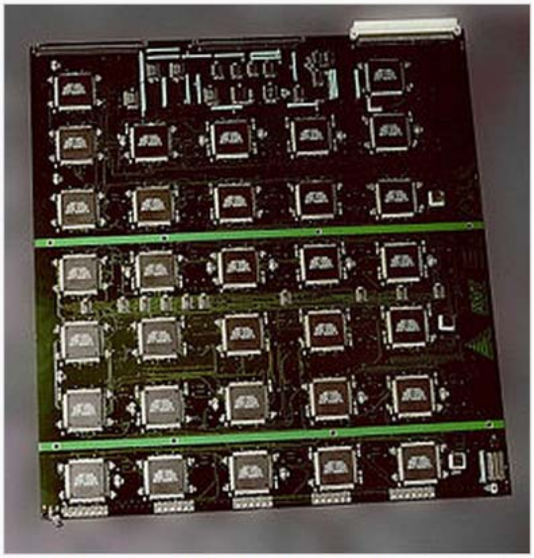
First Crypto War

64-bits

56 bits

error.

DES Cracking Machine



The EFF's US$250,000 DES cracking machine contained 1,856 custom chips and could brute force a DES key in a matter of days — the photo shows a two-sided DES Cracker circuit board fitted with 64 Deep Crack chips

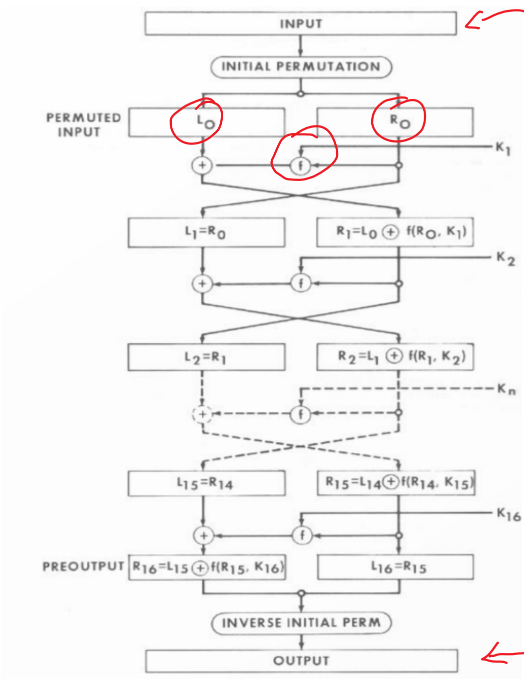
1998

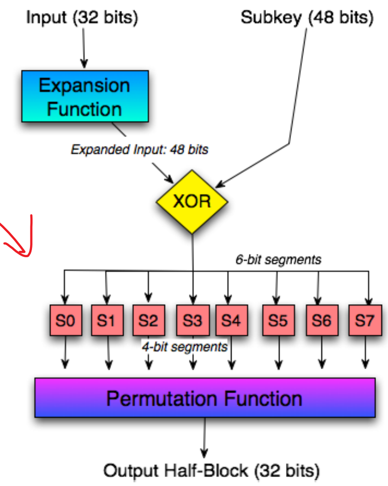
56

2^{56}

AES

DES Algorithm





SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

AES:
Advanced Encryption Standard

AES: Advanced Encryption Standard

NIST 2001

Rijndael ("Rain Doll")

~15

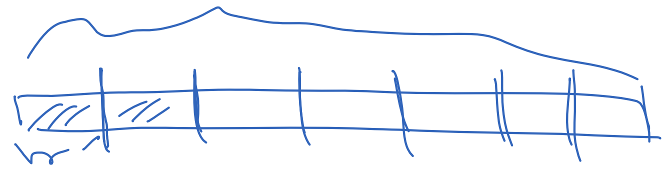
Key size. 128 192, or 256 bits

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

How to Encrypt Multiple Blocks

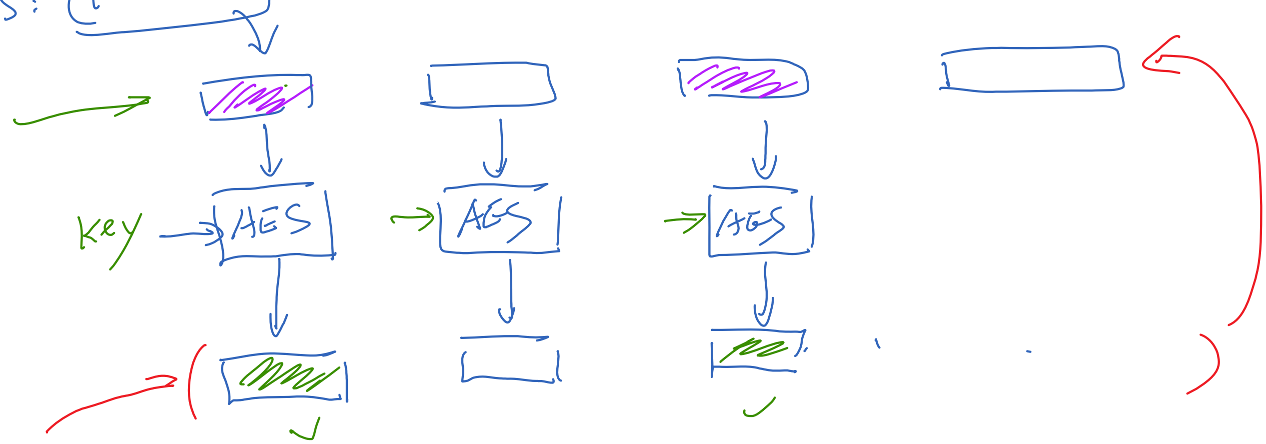
Encrypt More Than One Block

DES AES

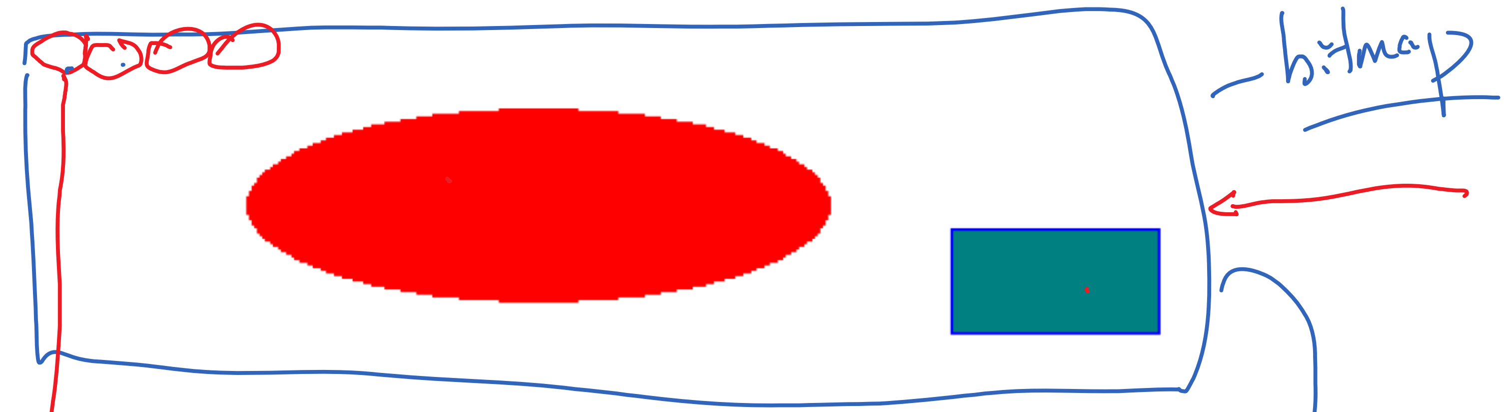


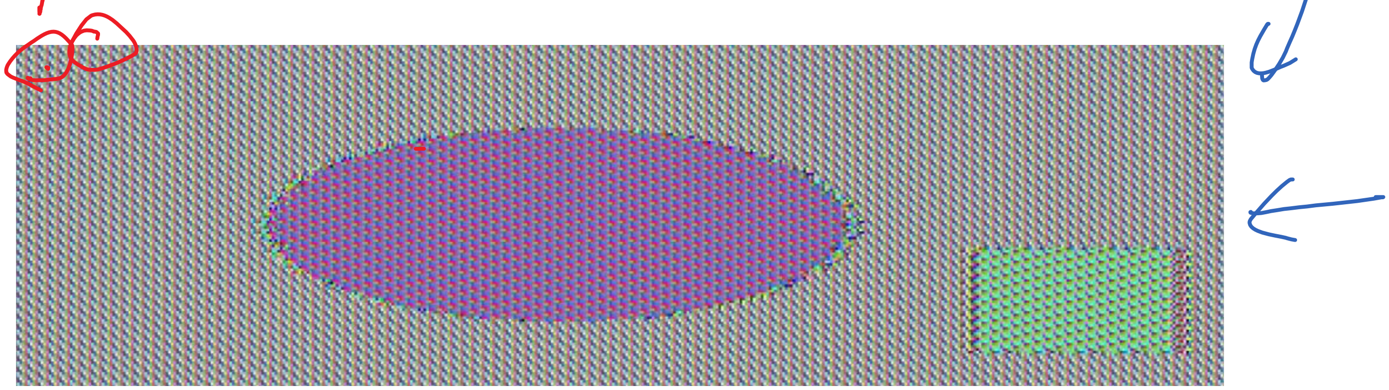
block Cipher:

{ DES: 64 bits
AES: 128 bits

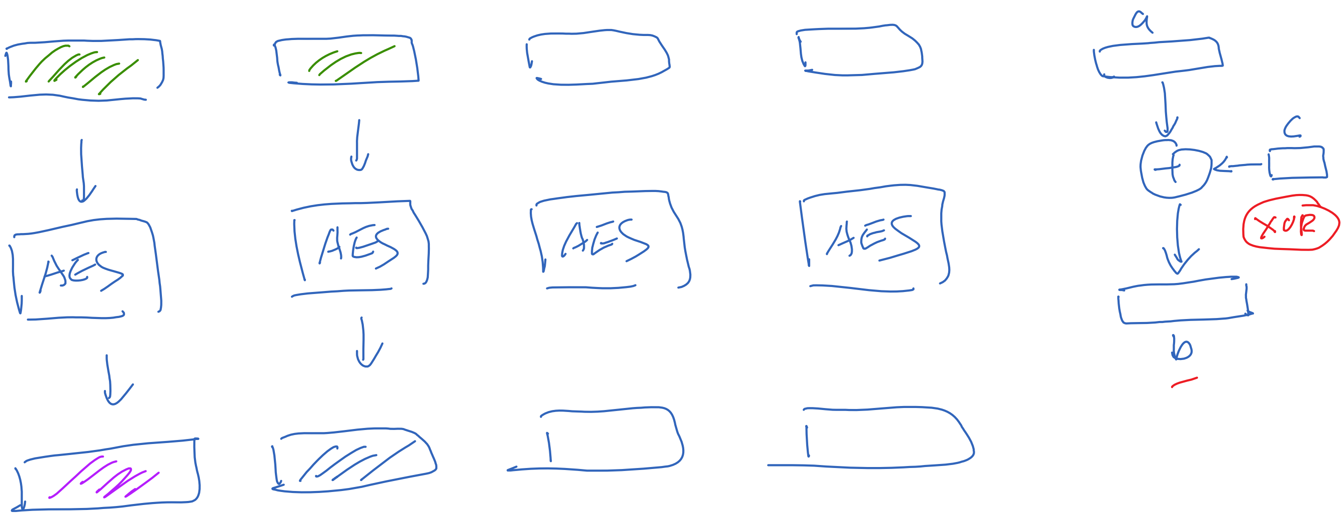


Result of a Simple Solution





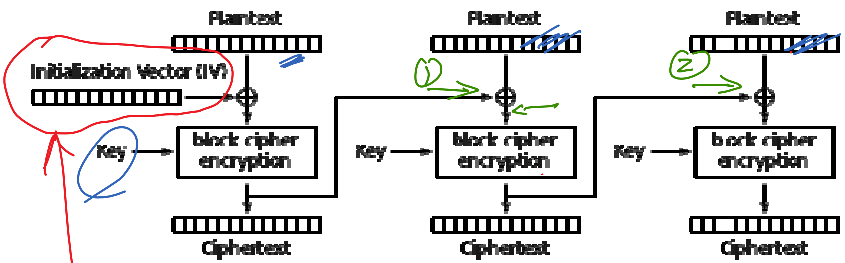
Question: Given the Building Blocks, Develop a Multi-Block Encryption Mode



SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

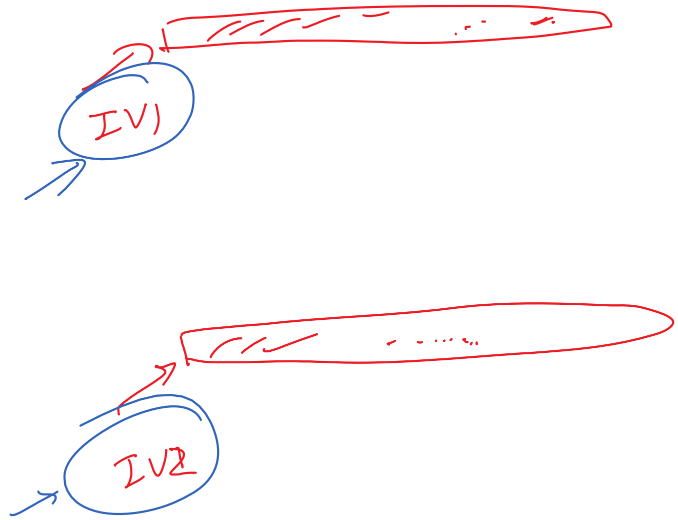
Encryption Modes

Cipher Block Chaining (CBC) Mode

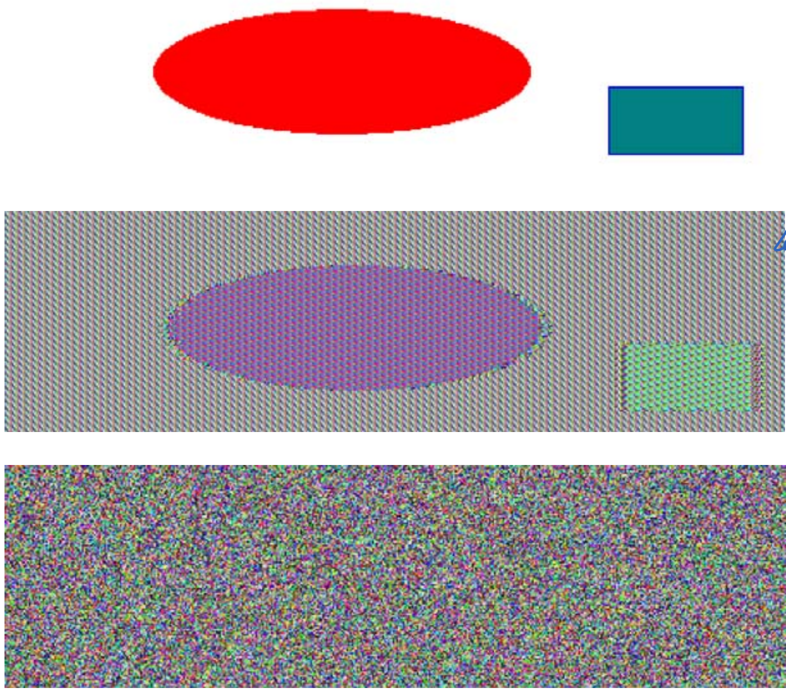


Cipher Block Chaining (CBC) mode encryption

random



ECB vs. CBC

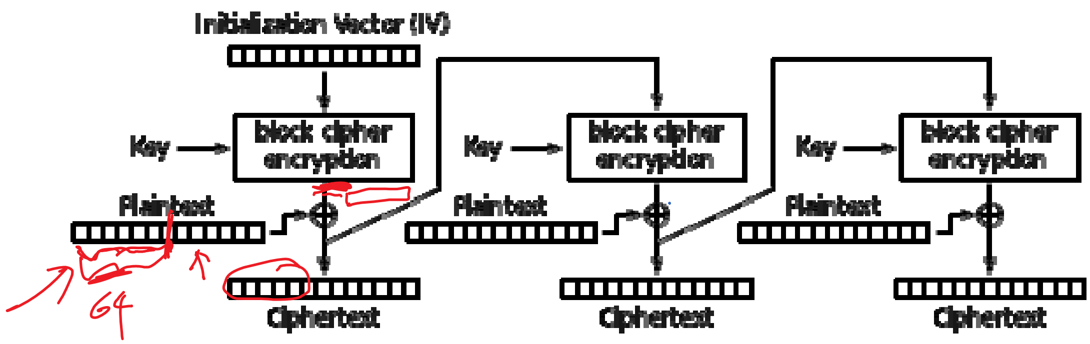


ECB

Electronic Code Book

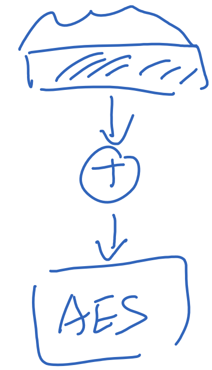
CBC

Cipher Feedback (CFB)

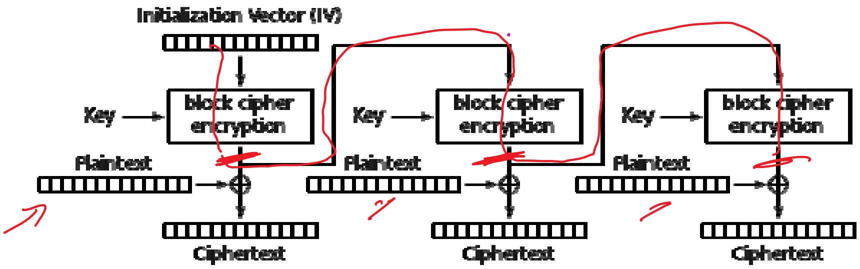


Cipher Feedback (CFB) mode encryption

Stream Cipher



Output Feedback (OFB)

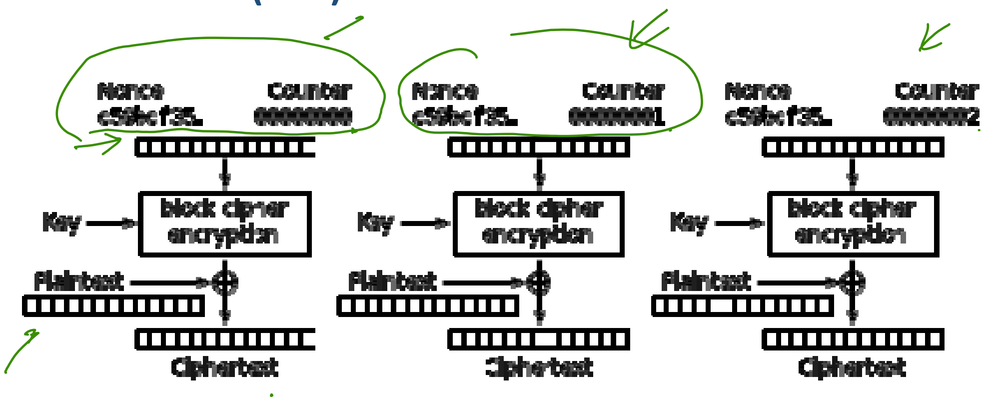


Output Feedback (OFB) mode encryption

Stream Cipher

parallel Encryption
↳ offline help

Counter Mode (CTR)

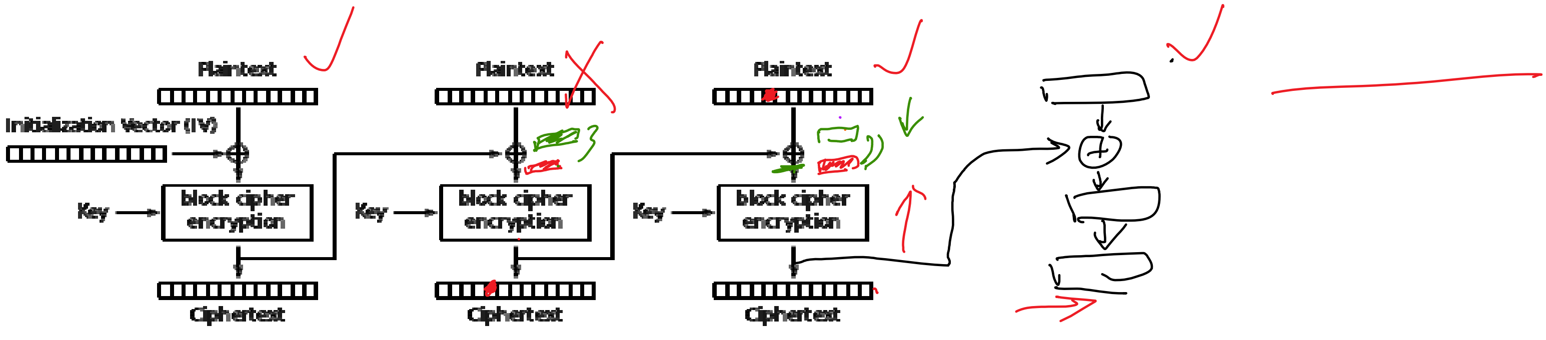


Counter (CTR) mode encryption

- Stream Cipher
- parallel Encryption

Question

During the transmission of the ciphertext, the fifth bit of the second block is corrupted. Without knowing that, the receiver decrypts the message. Please describe how much of the original plaintext the receiver can get. The diagram shows only 3 blocks, but assume there are 100 blocks of plaintext/ciphertext.

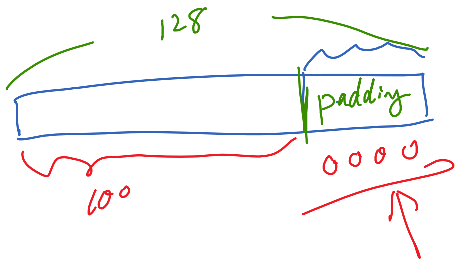


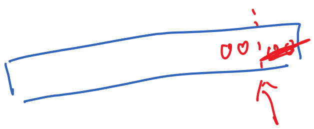
Cipher Block Chaining (CBC) mode encryption

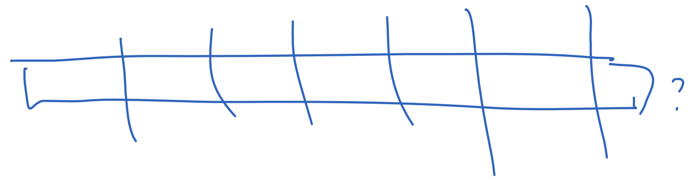
SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Padding

Padding







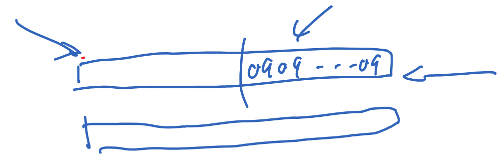
Padding: PKCS#5

9

```
Original plaintext 1:       0a23bac45092f7
Padded plaintext (PKCS#5):  0a23bac45092f70909090909090909

Original plaintext 2:       0a23bac45092f793273a7fe9093eaa88
Padded plaintext (PKCS#5):  0a23bac45092f793273a7fe9093eaa88
                            10101010101010101010101010101010
```

16



SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Random Number Generation

Why Do We Need Random Numbers?

Key

128 bit

Mistake: What Is the Mistake?

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

int main() {
 int c, n;

 printf("Ten random numbers in [1,100]\n");

 for (c = 1; c <= 10; c++) {
      n = rand()%100 + 1;
      printf("%d\n", n);
 }

 return 0;
}
```

rand( )

Generate Random Number (Another Try)

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

int main() {
 int c, n;

 printf("Ten random numbers in [1,100]\n");

 srand (time(NULL));

 for (c = 1; c <= 10; c++) {
      n = rand()%100 + 1;
      printf("%d\n", n);
 }

 return 0;
}
```

srand(random)

seed

rand()

time: # of seconds since 1970-01-01

32 bit

x 1000 000

60 x 60 = 3600

12 bit

56

128 bit

Attack on the Netscape Browser in 1996

```
RNG_CreateContext()
    (seconds, microseconds) = time of day; /* Time elapsed since 1970 */
    pid = process ID;  ppid = parent process ID;
    a = mklcpr(microseconds);
    b = mklcpr(pid + seconds + (ppid << 12));
     seed = MD5(a, b);
```

Where Do We Get True Randomness?

- user
  - mouse
  - Key stroke
- Hardware

Generate a Random 128-Bit Key

```
#define LEN 16 // 128 bits

unsigned char *key = (unsigned char *) malloc(sizeof(char)*LEN);
FILE* random = fopen("/dev/urandom", "r");
fread(key, sizeof(char)*LEN, 1, random);
fclose(random);
```

Use Special Hardware

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Summary

Summary

- ❖ Classical ciphers
- ❖ DES and AES
- ❖ Encryption modes
- ❖ Random number generation

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

One-Way Hash Function

A Game With Online Students

Student : A
Me : B

$\left.\begin{matrix} A \\ B \end{matrix}\right\}$ integer.

$A+B$ Even : Students win
$A+B$ odd : I win

Students send # first

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Concept of One-Way Hash

SYRACUSE UNIVERSITY ENGINEERING & COMPUTER SCIENCE

Concept

- Hash → fixed 160

$M \% 100 = 0 \dots 99$

Many → h

- One-way: $hash(M) = h$

Find M', s.t. $hash(M') = h$ is difficult.

- Collision Free: find M_1, M_2, $(M_1 \neq M_2)$, $hash(M_1) = hash(M_2)$

Algorithms

MD : Message Digest.

MD2 MD4 .. MD5 ✗

SHA : Secure Hash Algorithm.

SHA 0

SHA 1

SHA 2. ✓

256 bit. SHA-256

384 bit SHA-384

512 bit SHA-512

Application: Replay the Game

Question: Play the Game Again

Let's play the game again, this time using one-way hash function. Please describe how you would make the game fair for both sides.

- what property makes it fair to students?

  me?

Application: Replay the Game

Students:

O

B

Professor

O

hash(A)

A A'

B

A' ?

A. A'

$A \sim 0 \sim 10^6$

[random]

200 bit

one-way property

fair to professor.

hash(A) = hash(A')

Collision-free Property ✓

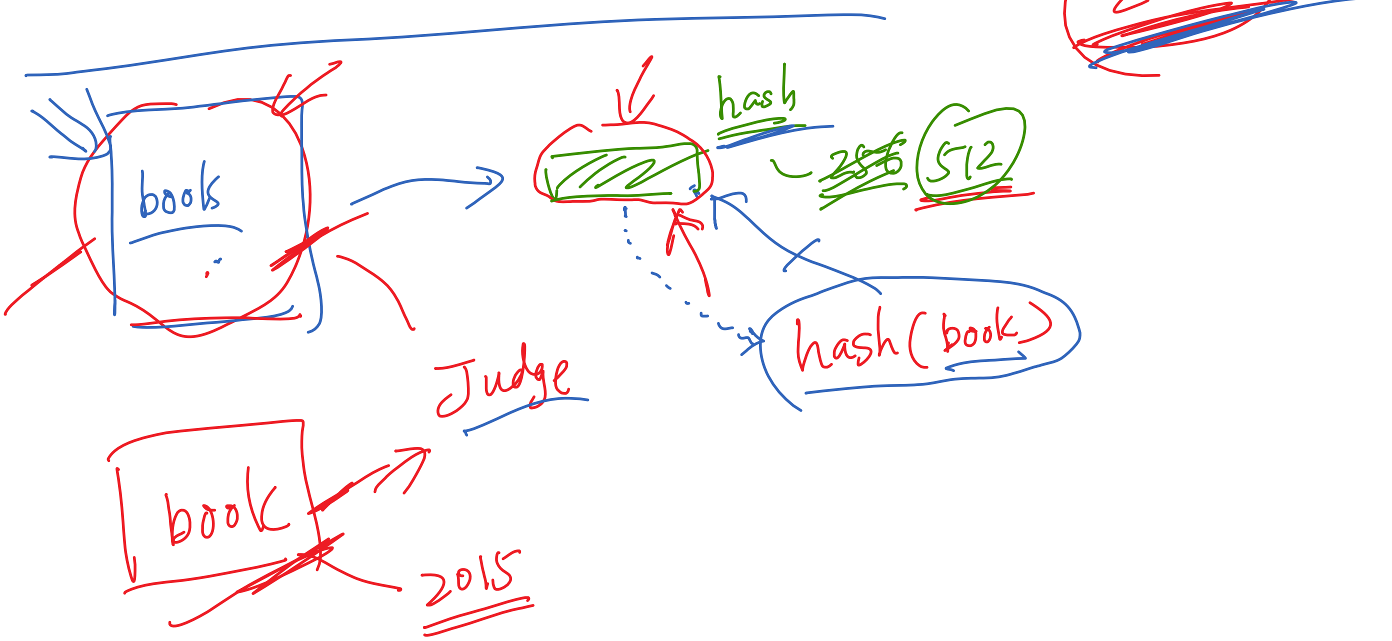
fair to students

More Applications

Application: Time Stamping

"Harry Porter"

J-K Rowling



Application: Password Authentication

username

password

file

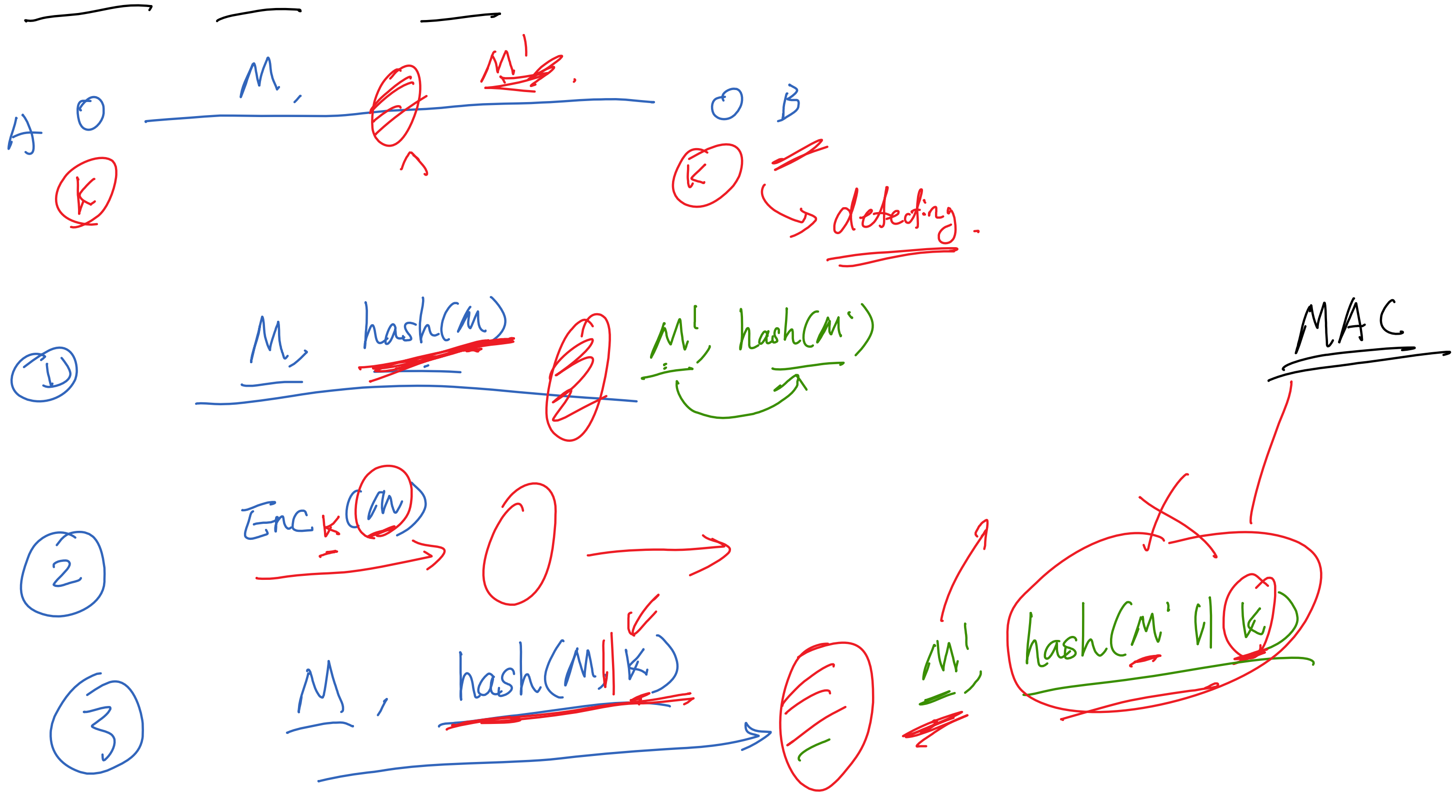
user
password :

one-way hash

passwd

Message Authentication Code

MAC: Message Authentication Code



HMAC

$$HMAC_K(m) = h((K \oplus opad) \;||\; h((K \oplus ipad)||m))$$

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Collision-Free Is Broken

Collision in MD5

```
Sequence #1
    d1  31  dd  02  c5  e6  ee  c4  69  3d  9a  06  98  af  f9  5c
    2f  ca  b5  87  12  46  7e  ab  40  04  58  3e  b8  fb  7f  89
    55  ad  34  06  09  f4  b3  02  83  e4  88  83  25  71  41  5a
    08  51  25  e8  f7  cd  c9  9f  d9  1d  bd  f2  80  37  3c  5b
    d8  82  3e  31  56  34  8f  5b  ae  6d  ac  d4  36  c9  19  c6
    dd  53  e2  b4  87  da  03  fd  02  39  63  06  d2  48  cd  a0
    e9  9f  33  42  0f  57  7e  e8  ce  54  b6  70  80  a8  0d  1e
    c6  98  21  bc  b6  a8  83  93  96  f9  65  2b  6f  f7  2a  70

Sequence #2
    d1  31  dd  02  c5  e6  ee  c4  69  3d  9a  06  98  af  f9  5c
    2f  ca  b5  07  12  46  7e  ab  40  04  58  3e  b8  fb  7f  89
    55  ad  34  06  09  f4  b3  02  83  e4  88  83  25  f1  41  5a
    08  51  25  e8  f7  cd  c9  9f  d9  1d  bd  72  80  37  3c  5b
    d8  82  3e  31  56  34  8f  5b  ae  6d  ac  d4  36  c9  19  c6
    dd  53  e2  34  87  da  03  fd  02  39  63  06  d2  48  cd  a0
    e9  9f  33  42  0f  57  7e  e8  ce  54  b6  70  80  28  0d  1e
    c6  98  21  bc  b6  a8  83  93  96  f9  65  ab  6f  f7  2a  70

 Both produce MD5 digest 79054025255fb1a26e4bc422aef54eb4
```

A , B

hash(A) = hash(B)

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Summary

Summary

- One-way hash function
  - One-way property
  - Collision-free property
- Algorithms
- Applications
  - Online game
  - Time stamping
  - Message authentication code
  - HMAC

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE