Collision

Venn diagram: "preimg resistant", "2nd preimg resistant", "collision resistant"

Secure Hash Code

Y_0, Y_1, ... Y_{L-1}
$IV = C_0 \rightarrow$ F ... F ... F C_{L-1}

AES Example:-
Plaintext: ·· — — — —
key :- — — — —
Ciphertext: - — —

Digital Signature Process
Bob signs msg

msg M → cryptography Hash function → h → Digital signature generating algo → msg M | S

Bob's Privat key

Alice

msg m | S → // → h → // → return valid/ invalid signature.

Groups
Abelian Grup
Ring
Cumulative b...
Integral
Field
Finite Field

AES Key expansion.

key Expansion (Byte key[16] word w[44])

{word temp

```
for (i=0; i<4; i++)  w[i] = {key[4*i]
                              key[4*i+1]
                         .    key[4*i+3]


for(i=9; i<44; i++)
{temp = w[i-1];
    if (i mod 4=0)  temp = SubWord [RodWord (temp)]
                          ⊕ Rcon [i/4];
    w[i] = w[i-4] ⊕ temp
}
```
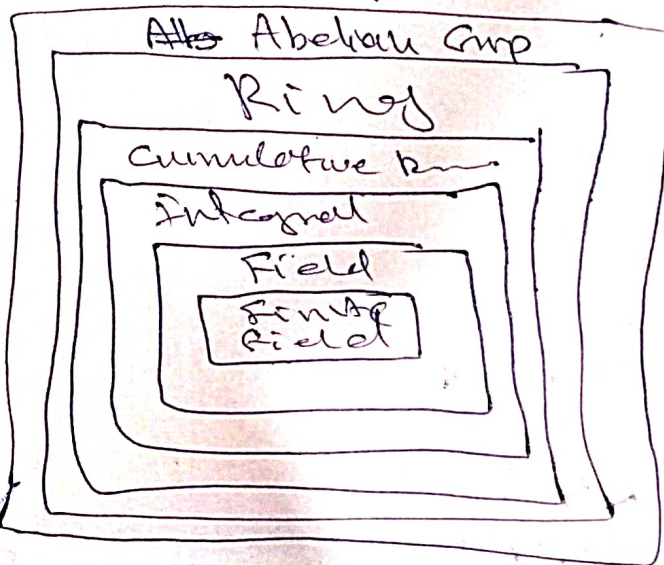
Madel of Network. Secur.

3d party

Euclidean Algo.

```
start
```

No ← | a > b | → Yes → | divide a/b | ← | swap b with r |

| swap a with b |

No ← | R > 0 | → Yes → | swap a with b |

| It is the GCD of the value |

Stream Cipher

| Stream bit cipher generation algorithm |
key → (+)

plain text →

encryption

cipher text

↓

key →
| bit ___ |
(+)
decr___

plain text

Block - cipher

| plain text | → | cipher text |
↓ ↓
k → | encryption | key → | Decryption |
↓ ↓
| cipher text | | plain text |

16 Byte input

Input state

Rand(0) key

key - N Byte

(N byte)

initial transformation

after initial transform

Round 1
(4 transformation)

Round(1) output state (16 byte)

Round 1 key

Round(1) output state (16 byte)

Round 2
(4 transformation)

Round 2 key

Round N-1 output

N-1
(4 transformation)

Round N-1 key

Round N
3 transformation

Round N key

Key expansion

Round N

final state

16 byte cipher text

AES encryption process

in0	in4	in8	in12
in1	in5	in9	in13
in2	in6	in10	in14
in3	in7	in11	in15

①

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	//	/	//
$S_{2,0}$	//	//	//
$S_{3,0}$	//	/	//

②

input, state array, output
AES.

③

⑤

k_0	k_4	0	
k_1	//		
k_2	//		
k_3			

key

| w_0 | w_1 | w_2 | ... | w | w | w_{43} |

key expansion

AES Structure

Input (plaintext)

LE₀ | RE₀

Round 2

LE₁ | RE₁

⊕ → k

LE₁₆ | RE₁₆

F

LE₁₇ | RE₁₇

LE₁₈ | RE₁₈

FEISTEL Encryption.

400/2 = 800/2
20 = 2

40 rounds

RD 17 = LE₀ | LD 17 = RE₀

LD₁₆ = RE₀ | RD₁₆ = LE₀

LD₂ = RE₁₄ | RD₂ = LE₁₄

F key 15

LD₁ = RE₁₅ | RD₁ = LE₁₅

F key 16

LD₀ = RE₁₆ | RD₀ = LE₁₆

FEISTEL Decryption

64 bit Plaintext

Initial Permutation

Round 1

Round 2

Round 16

swap 32 bit

Inverse initial Permutation

64 bit cipher text

64-bit key

Permuted choice 1

56

Permuted choice 2 ← 56 ← left shift circular

56

" " " ← 56 ← "

" " " ← 56 ← "

56

56

DES Algorithm