An Toàn Và Bảo Mật Thông Tin

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

1. Giá trị Hàm Euler.

n	$\emptyset(n)$	Điều kiện
p	p-1	p là nguyên tố
p^t	$p^t - p^{t-1}$	p là số nguyên tố
s.t	$\emptyset(s).\emptyset(t)$	gcd(s,t) = 1
p.q	(p-1).(q-1)	p,q là số nguyên tố

2. Định lý ferma.

5.1. Định lý Ferma

- ***Cho p là số nguyên tố, khi đó:***
  - ***Nếu a là số nguyên dương và GCD(a, p) = 1, thì:***

$$a^{p-1} \pmod p = 1$$

  - ***Nếu a là số nguyên dương bất kỳ thì:***

$$a^p \pmod p = a \pmod p$$

3. Định Lý Euler.

5.2. Định lý Euler

- Định lý Euler (Tổng quát hoá của Định lý Ferma):
  - ***Cho a,n là hai số nguyên tố cùng nhau, tức là gcd(a,n)=1. Khi đó***

$$a^{\emptyset(n)} \pmod n = 1$$

  - ***Nếu a và n là hai số nguyên bất kỳ (không cần nguyên tố cùng nhau), khi đó:***

$$a^{\emptyset(n)+1} \equiv a \pmod n$$

4. Căn nguyên thủy + Logarit rời rạc.

Căn nguyên thủy (căn nguyên tố)

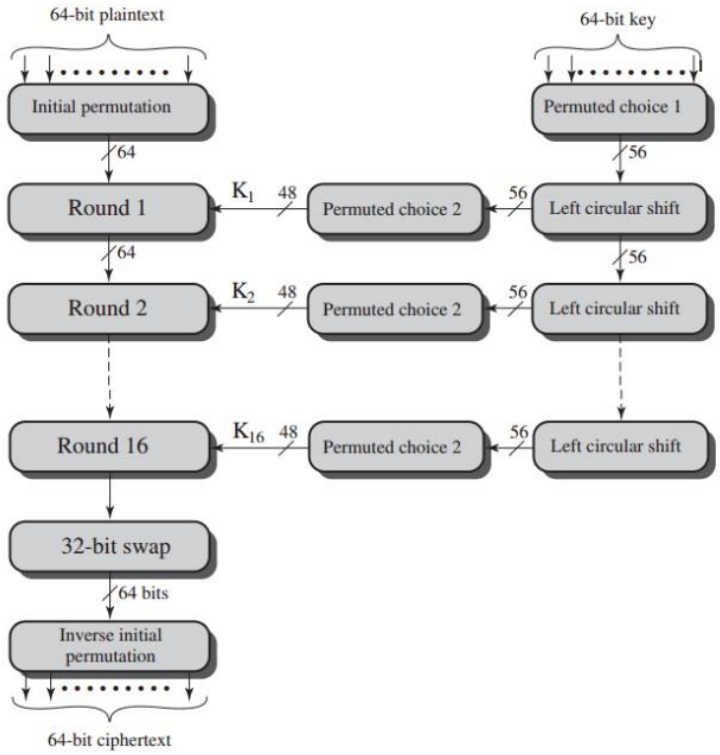
- ***Định Nghĩa*: Xét m để a^m mod n = 1. Nếu giá trị m = Φ(n) là số dương nhỏ nhất thoả mãn công thức trên thì a được gọi là căn nguyên thủy của n.**
- Từ Định lý Euler: $a^{\phi(n)}$ mod n=1, với GCD(a,n)=1
- ***Định lý*: a là căn nguyên thủy của n, nếu a nguyên tố cùng nhau với n và a^m mod n ≠ 1, nếu 0<m < ø(n)**

Logarit rời rạc

- *Dễ thấy, với số nguyên b bất kỳ, nếu a là căn nguyên thủy của số nguyên tố n, thì luôn tồn tại duy nhất 1 số m (0 ≤ m ≤n-1) sao cho b≡a^m (mod n)*
- ***ĐN: Với số nguyên b bất kỳ, Số m thỏa mãn $b \equiv a^m (mod\ n)$ với $0 \leq m \leq (n-1)$ được gọi là logarit rời rạc của b với cơ số a theo modulo n***
- Kí hiệu $\mathbf{m} = dlog_{a,n}(b) = dlog_a\ b(mod\ n)$

5. DES.

Tổng quan của thuật toán mã hóa DES



Hoán vị khởi đầu của DES

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Bảng 1

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

Bảng 2

M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5
M_{63}	M_{55}	M_{47}	M_{39}	M_{31}	M_{23}	M_{15}	M_7

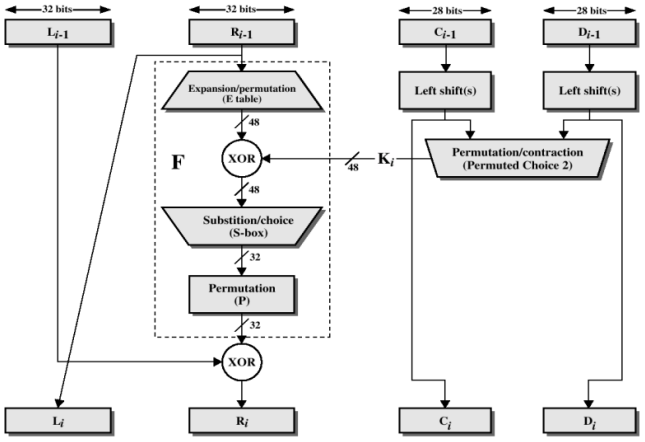


Figure 2.4 Single Round of DES Algorithm

(c) Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

- 8 Sbox:

S1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	0	14	2	13	6	15	0	9	10	4	5	3

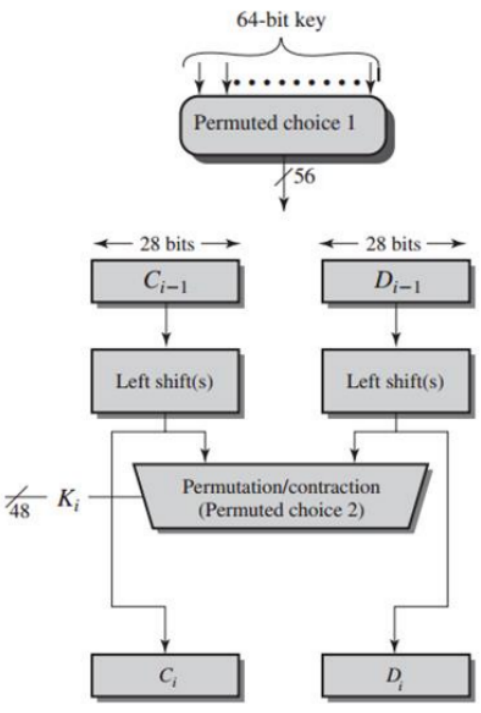
S6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Sinh khóa

- Đầu vào của khóa là khối 64 bít
=>bỏ 8 bít ở vị trí bội của 8
=> được key 56 bit
- Thực hiện phép hoán vị
  Permuted Choice 1
- Chia thành 2 nửa 28 bit
- Thực hiện Left shift với mỗi nửa
  dịch chuyển trái 1 hoặc 2 bít
  dựa vào bảng shift cho mỗi
  vòng
- Hoán vị choice 2 =>48 bit



(a) Input Key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

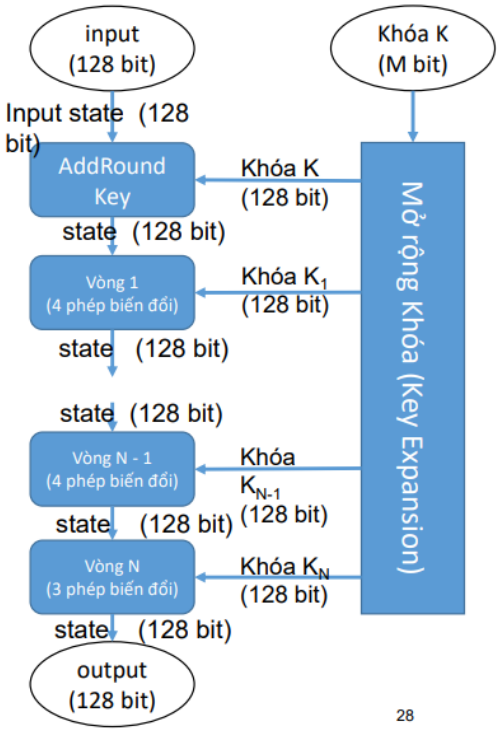
6. AES:

Cấu tạo chuẩn mã nâng cao AES

Chi tiết một vòng lặp
(từ vòng 1 đến N – 1)

1. **Substitute bytes**
2. **ShiftRows**
3. **MixColumns**
4. **AddRoundKey**

Riêng vòng thứ N không có phép **MixColumns.**



Số vòng lặp (N)	10	12	14
Khóa (bit)	128	192	256
Input (bit)	128	128	128
Khóa vòng lặp (bit)	128	128	128
Khóa mở rộng (bytes)	176	208	240

Phép *SubBytes*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

- Phép ***SubBytes*** thay thế mỗi byte trong state bằng 1 byte trong bảng **S-box**.
- Ví dụ:

  Byte {95} được thay thế thành {2A} (giá trị tại hàng 9, cột 5 của bảng S-box)

  ➔SubBytes({95}) = {2A}

  ➔SubByte({59}) = {CB}

Phép MixColumns

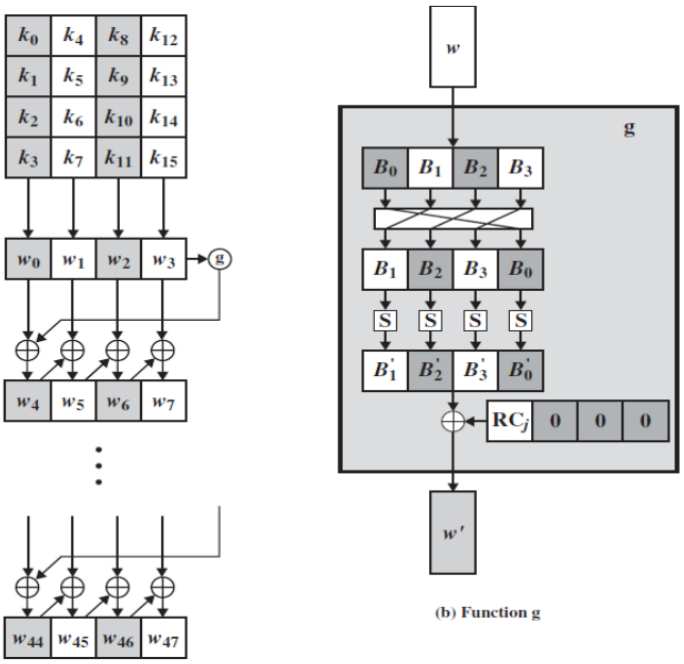
- **MixColumns** được định nghĩa bằng phép nhân ma trận sau

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

$$s'_{0,j} = (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$
$$s'_{1,j} = s_{0,j} \oplus (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j}$$
$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j})$$
$$s'_{3,j} = (3 \bullet s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \bullet s_{3,j})$$

- Các phép toán thực hiện trong GF(2^8)

Mô hình mở rộng khóa



(b) Function g

Mở rộng khóa AES

- **Rcon** là một word (4 bytes):
- Rcon[j] = (RC[j], 0, 0, 0), với RC[1] = 1, RC[j] = 2*RC[j-1] với phép nhân được định nghĩa trên trường GF(2^8).
- Các giá trị của RC[j] trong cơ số 16 là:

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

7. RSA:

Khởi tạo khóa RSA

1. Sinh khóa (Alice)	Ví dụ
Chọn p, q là hai số nguyên tố khác nhau	p = 17 & q = 11
Tính n = pq	n = pq =17 x 11=187
Tính $\phi(n) = (p-1)(q-1)$	ø(n) = 16x10=160
Chọn số nguyên e, gcd ($\phi(n)$, e) = 1; 1 <e < $\phi(n)$	Chọn e = 7 thỏa mãn gcd(e,160)= 1
Tính $d \equiv e^{-1} \pmod{\phi(n)}$	d = 23 vì: 23x7(mod 160)=161 mod 160=1
Khóa công khai: PU = {e, n}	PU = {7,187}
Khóa riêng: PR = {d, n}	PR = {23,187}

Mã hóa và Giải mã với RSA

2. Bob mã hóa với khóa công khai của Alice	
Bản rõ	M < n
Bản mã	$C = M^e \bmod n$

Ví dụ
M = 88
$C = 88^7 \bmod 187 = 11$

3. Alice giải mã bằng khóa riêng của Alice	
Bản mã	C
Bản rõ	$M = C^d \bmod n$

Ví dụ
C = 11
$M = 11^{23} \bmod 187 = 88$

8. Diffie-HellMan:

Thuật toán Diffie – Hellman và ví dụ

1. Các giá trị công khai chung
q là số nguyên tố
a là một căn nguyên thủy của q, a < q

Ví dụ
q =353
a = 3

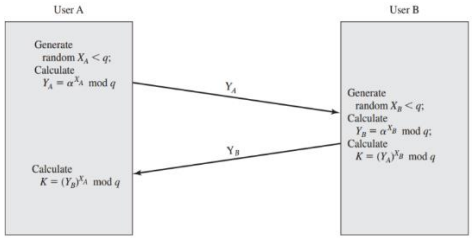
2. Alice tạo khóa
Chọn khóa riêng $X_A < q$
Tính khóa công khai $Y_A = a^{XA} \bmod q$

Ví dụ
$X_A = 97$
$Y_A = 3^{97} \bmod 353 = 40$

2. Bob tạo khóa
Chọn khóa riêng $X_B < q$
Tính khóa công khai $Y_B = a^{XB} \bmod q$

Ví dụ
$x_B = 233$
$y_B = 3^{233} \bmod 353 = 248$

Trao đổi khóa Diffie-Hellman



- $K = \alpha^{X_A . X_B} \bmod q = ?$ **160**
- K được sử dụng như khóa phiên (khóa bí mật chung)

9. Mật mã Elgaman

Mật mã Elgaman

- Được đề xuất bởi T.Elgaman năm 1984
- Mã Elgaman được dùng trong chuẩn chữ ký số (Digital Signature Standard – DSS) và email standard S/MIME

1. Các giá trị công khai chung
q Là số nguyên tố
a là một căn nguyên thủy của q (a < q)

Ví dụ
q = 19
a =10

2. Alice tạo khóa
Chọn $X_A < q - 1$
Tính $Y_A = a^{XA} \bmod q$
Khóa công khai: PU = {q, a, Y_A}
Khóa riêng: X_A

Ví dụ
$X_A = 5$
$Y_A = a^5 \bmod 19 = 3$
{19, 10, 3}
5

Mật mã Elgaman

3. Bob muốn gửi tin nhắn cho Alice
Bản gốc: M < q
Chọn ngẫu nhiên k < q
Tính $K = (Y_A)^k \bmod q$
Tính $C_1 = a^k \bmod q$;
Tính $C_2 = KM \bmod q$
Bản mã: (C_1, C_2)

Ví dụ
M = 17
k = 6
$K = 3^6 \bmod 19 = 7$.
$C_1 = 10^6 \bmod 19 = 11$
$C_2 = 7 \times 17 \bmod 19 = 5$
(11, 5)

4. Alice giải mã tin nhắn từ Bob
Bản mã: (C_1, C_2)
Tính $K = (C_1)^{XA} \bmod q$
Bản rõ: $M = (C_2 K^{-1}) \bmod q$

Ví dụ
(11, 5)
$K = 11^5 \bmod 9 = 7$.
$7^{-1} \bmod 19 = 11$. $M = 5 \times 11 \bmod 19 = 17$.

10. Chữ Ký Điện Tử DSS.

Thuật toán chữ ký điện tử (DSA)
(Digital Signature Algorithm)

1. Các giá trị công khai chung
p: số nguyên tố trong đó $2^{L-1} < p < 2^L$, với $512 \le L \le 1024$ và L là một bội số của 64;
q: Ước số nguyên tố của (p – 1), q có độ dài 160 bit
$g = h^{(p-1)/q} \bmod p$, trong đó h là số nguyên $1 < h < (p-1)$ sao cho $h^{(p-1)/q} \bmod p > 1$.

3. Ký chữ ký số
$r = (g^k \bmod p) \bmod q$ $s = [k^{-1}(H(M) + xr)] \bmod q$ Chữ ký số = (r, s)

2. Người dùng
Khóa riêng: x thỏa $0 < x < q$
Khóa công khai: $y = g^x \bmod p$
Số bí mật cho mỗi tin nhắn: k thỏa $0 < k < q$

Kiểm chứng chữ ký DSA
DSA Signature Verification

Đầu vào cho xác minh	4. Xác minh chữ ký
M: tin nhắn được ký H(M): mã băm của M sử dụng SHA-1 M', r', s': là các phiên bản nhận được của M, r, s.	$w = (s')^{-1} \bmod q$ $u_1 = [H(M')w] \bmod q$ $u_2 = (r')w \bmod q$ $v = [(g^{u1} y^{u2}) \bmod p] \bmod q$ Kiểm tra: v = r'

11. Chữ ký số ElGamal.

Chữ ký số ElGamal

1. Các giá trị công khai chung	Ví dụ
q là số nguyên tố	q = 19
a là một căn nguyên thủy của q (a < q).	a = 10

2. Người gửi tạo khóa	Ví dụ
Chọn $X_A < q - 1$	$X_A = 16$
Tính $y_A = a^{XA} \bmod q$	$Y_A = 10^{16} \bmod 19 = 4$
Khóa công khai PU = {q, a, Y_A}	{19, 10, 4}
Khóa riêng X_A	16

Thực hiện ký (Elgamal)

3. Người gửi kí vào M	Ví dụ
Tính m = H(M); $0 \le m \le q-1$	m = H(M) = 14
Chọn K, Gcd(K,q-1) = 1 và $0 \le K \le q-1$	K = 5, gcd(5, 18) = 1
Tính $S_1 = a^K \bmod q$;	$S_1 = 10^5 \bmod 19 = 3$
Tính $K^{-1} \bmod (q - 1)$	$5^{-1} \bmod 18 = 11$
Tính $S_2 = K^{-1}(m - X_A S_1) \bmod (q - 1)$	$S_2 = 11(14 - 16*3) \bmod 18 = 4$
Chữ ký số (S_1, S_2)	(3, 4)

Xác minh chữ ký (Elgamal)

4. Người nhận xác minh chữ ký của người gửi	Ví dụ
Chữ ký nhận được (S_1, S_2)	(3, 4)
Tính $V_1 = a^m \bmod q$	$V_1 = 10^{14} \bmod 19 = 16$
Tính $V_2 = (Y_A)^{S1}(S_1)^{S2} \bmod q$	$V_2 = 4^3 * 3^4 \bmod 19 = 16$
Nếu $V_1 = V_2$ thì chữ ký là hợp lệ.	chữ ký số là hợp lệ