- **RSA**

In RSA textbook

User A keys are $SK_a = (p_A, q_A, d_A) = (5, 11, 23)$ and $pK_A = (n_A, e_A) = (55, 7)$

User B keys are $SK_b = (p_B, q_B, d_B) = (3, 5, 7)$ and $pK_B = (n_B, e_B) = (21, 5)$

A wants to send to B a signed message M. So she encipher $C = Enc_{pk_B}(M)$, compute her digital signature σ as the pair $\sigma = (Enc_{pk_B}(F), h(M))$ where $F = Enc_{sk_A}(h(M))$

Assuming $h(M) = 18$ find the digital signature i.e. the pair $(Enc_{pk_B}(F), h(M))$

OPEN ANSWER:

Calcolo F come $h(M)^{d_A} \bmod (p_A \cdot q_A) \Rightarrow 18^{23} \bmod 55 = 2$

Trovo $Enc_{pk_B}(F)$ come $F^{e_B} \bmod (p_B \cdot q_B) \Rightarrow 2^5 \bmod 21 = 11$

$\sigma = (Enc_{pk_B}(F), h(M)) = (11, 8)$

- **Intersezione**

Let $E: y^2 \equiv x^3 + 2x + 2 \bmod 17$ an ellptic curve and let $P=(6,3)$ and $Q=(10,6)$ and $R=(x,y)$ such that $P+Q+R=\phi$

a) $R = (9,16)$

b) $R = (9,1)$ ✓

c) $R = (9,14)$

d) $R = (9,12)$

Verifico P e Q

$P \Rightarrow 3^2 = (6^3 + 2 \cdot 6 + 2) \bmod 17 = 230 \bmod 17 = 9$

$Q \Rightarrow 6^2 = (10^3 + 2 \cdot 10 + 2) \bmod 17 = 1022 \bmod 17 = 36 \bmod 17 = 2 \bmod 17$

$P \oplus Q = -R(x_3, y_3)$

$= (\lambda^2 - x_1 - x_2, -(\lambda x_3 + v))$

$= (25 - 6 - 10, -(5 \cdot 9 + 7))$

$= (9, -(52 \bmod 17))$

$= (9, -(1))$

$R = (x_3, -y_3) = (9, 1)$ ✓

$\lambda = \frac{6-3}{10-6} = \frac{3 \bmod 17}{4 \bmod 17}$

$= 3 \bmod 17 \cdot (4 \bmod 17)^{-1}$

Eulero Fermat

$= 3 \cdot 13 = 39 \bmod 17 = 5$

$v = y_1 - \lambda x_1$

$= y_1 - \lambda x_1$

$= 3 - 5 \times 6$

$= -27 \bmod 17 = 7$

- Algoritmo di Euclide

Find $x \in \mathbb{Z}_{401}$ such that

$x \cdot 56 \equiv 1 \bmod 401$ and
$5 \cdot x \equiv 308 \bmod 401$

Solution: we have to find the inverse of 56

Extended Euclidean Algorithm

$401 = 56 \times 7 + 9$
$56 = 9 \times 6 + 2$
$9 = 2 \times 4 + 1$
$2 = 1 \times 2 + \emptyset$

$p_0 = 0$
$p_1 = 1$

$p_i = p_{i-2} - q_{i-2} p_{i-1} \bmod N$

$p_2 = 0 - 7 \times 1 \bmod 401 = 394$

$p_3 = 1 - 6 \times 394 \bmod 401 = 1 - 359 \equiv 43 \bmod 401$

$p_4 = 394 - 43 \times 4 \bmod 401 = 222$

Try: $5 \times 222 = 1110 \equiv 308$ OK!

So $x \equiv 222 \bmod 401$

EXPANDED

$x \cdot 56 = 1 \bmod (401)$

$x = \frac{1}{56} \bmod (401)$

$401 = 56 \cdot 7 + 9$

$56 = 9 \cdot 6 + 2$

$9 = 2 \cdot 4 + 1$

$1 = 9 - 2 \cdot 4$

$1 = 9 - (56 - 9 \cdot 6) \cdot 4$

$= 9 - 56 \cdot 4 + 9 \cdot 24$

$= -56 \cdot 4 + 9 \cdot 25$

$= -56 \cdot 4 + (401 - 56 \cdot 7) \cdot 25$

$= -56 \cdot 4 + 401 \cdot 25 - 56 \cdot 175$

$= -56 (179) \Rightarrow \frac{1}{56} = -179$

$x = 222 \bmod 401$

• Equation Solution

Let $p = 11$, $q = 19$, $n = pq = 209$

How many solution does the equation $x^2 \equiv 171 \bmod 209$ have?

a) 1

b) 3

c) $\emptyset$ ✓

d) 4

e) 2

Solution: Let p be a prime and r an integer not divisible by p. Then r is a quadratic residue mod p iff

$$r^{\frac{p-1}{2}} \equiv 1 \bmod p$$

The group of all quadratic residues is $1^2, 2^2, 3^2, \dots \left(\frac{p-1}{2}\right)^2$

Let $x^2 \equiv r \bmod n$

If $r = 0$, then $\exists!\ x \equiv 0 \bmod n$

If $r > 0$:

Use CRT to split the equation in other 2nd degree equations $x^2 \equiv a \bmod p^k$ with p odd and $\gcd(a, p) = 1$

- NO SOLUTIONS if $\left(\frac{a}{p}\right) = -1$ (if a is not a quadratic residue mod p
- 2 SOLUTIONS x_1, x_2 if $\left(\frac{a}{p}\right) = 1$ (if a is a quadratic residue mod p)
- $x^2 \equiv a \bmod 2^k$:
  - if $k = 1$ $\Rightarrow$ UNIQUE solution $x \equiv 1 \bmod 2$
  - $k = 2 \Rightarrow$ no solution if $a = 3$ or there are 2 solutions $x_1 \equiv 1 \bmod 4$ and $x_2 \equiv 3 \bmod 4$ if $a \equiv 1 \bmod 4$
  - $k = 3 \Rightarrow$ no solution if $a \equiv 1 \bmod 2^k$ or there are 4 solutions $x_1, -x_1, x_1 + 2^{k-1}, -(x_1 + 2^{k-1})$ if $a \equiv 1 \bmod 2^3$

In this case we exploit $209 = 19 \times 11 \Rightarrow$ CRT

$$\begin{cases} x^2 = 171 \equiv 6 \bmod 11 \\ x^2 = 171 \equiv 0 \bmod 19 \end{cases} \Rightarrow \exists!\ x \equiv 0 \bmod 19$$

If we substitute $\Rightarrow 0 \neq 6 \bmod 11$

$\Rightarrow$ NO SOLUTIONS!

Es 1 other version

$p=11,\ q=19,\ pq=209$

How many solutions does $x^2 \equiv 130 \bmod 209$ have?

a) 1

b) 4 ✓

c) 2

d) 3

e) $\emptyset$

Solution: use CRT to split the equation

$$\begin{cases} x^2 \equiv 9 \bmod 11 \\ x^2 \equiv 16 \bmod 19 \end{cases}$$

$$\begin{cases} x \equiv \pm 3 \bmod 11 \\ x \equiv \pm 4 \bmod 19 \end{cases}$$

Check if they are quadratic residues

$9^{\frac{11-1}{2}} \equiv 1 \bmod 11$? $\Rightarrow 9^5 = 9^2 \cdot 9 \cdot 9^2 = 4 \cdot 4 \cdot 9 = 5 \cdot 9 \equiv 1 \bmod 11$ OK

$16^{\frac{19-1}{2}} \equiv 1 \bmod 19$? $\Rightarrow 16^9 = 16^2 \cdot 16^2 \cdot 16^2 \cdot 16^2 \cdot 16 = 9 \cdot 9 \cdot 9 \cdot 9 \cdot 16$

$= 5 \cdot 5 \cdot 16 = 6 \cdot 16 = 6 \cdot 4 \cdot 4 \equiv 1 \bmod 19$ OK

Find solution with CRT

$f: \mathbb{Z}_{11} \times \mathbb{Z}_{19} \to \mathbb{Z}_{209}$

$a(f(1,0)) + b(f(0,1)) = 133x + 77y$

$\begin{cases} a = 1 \bmod 11 \\ a = 0 \bmod 19 \end{cases}$

$a = k \cdot 19 = 7 \cdot 19 = 133$

$b = k \cdot 11 = \dots = 77$

$k \cdot 19 = 1 \bmod 11$

$k = 19^{-1} \bmod 11$

ø	$11 = 19 \cdot 0 + 11$	$p_0 = 0$
1	$19 = 11 \cdot 1 + 8$	$p_1 = 1$
2	$11 = 8 \cdot 1 + 3$	$p_2 = 0 - 1 \cdot 0 = 0$
3	$8 = 3 \cdot 2 + 2$	$p_3 = 1 - 0 \cdot 1 = 1$
4	$3 = 2 \cdot 1 + 1$	$p_4 = 0 - 1 \cdot 1 = 10 \bmod 11$
		$p_5 = 1 - 10 \cdot 2 = -19 \bmod 11 = 3$
		$p_6 = 10 - 3 \cdot 1 = 7$

esplicito le soluzioni

$\pm 3 \begin{cases} 3 \bmod 11 \\ 8 \bmod 11 \end{cases}$

$\pm 4 \begin{cases} 4 \bmod 19 \\ 15 \bmod 19 \end{cases}$

Provo le 4 combinazioni

$(3,4) = 3 \cdot 133 + 4 \cdot 77 = 80$

$(3,15) = 3 \cdot 133 + 15 \cdot 77 = 15$

$(8,4) = 8 \cdot 133 + 4 \cdot 77 = 118$

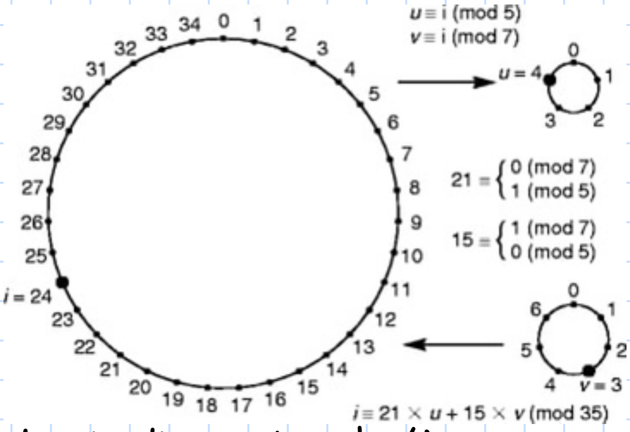
$(8,15) = 8 \cdot 133 + 15 \cdot 77 = 169$

Trovate le 4 soluzioni

Isomorfismo CTR

Let $f: \mathbb{Z}_3 \times \mathbb{Z}_5 \rightarrow \mathbb{Z}_{15}$ be the isomorphism of CRT, then

a) $f(x,y) = 7x + 9y$
b) $f(x,y) = 6x + 10y$
c) $f(x,y) = 10x + 6y$ ✓
d) $f(x,y) = 12x + 4y$



Solution:

CRT: Assume n_1, n_2 coprime, i.e $\gcd(n_1, n_2) = 1$. Let x be the solution to the following systems of modulo identities

$x \equiv a_1 \bmod n_1$
$x \equiv a_2 \bmod n_2$

Then $x = (X_2 n_2 a_1 + X_1 n_1 a_2) \bmod N$, where $N = n_1 \times n_2$ and $X_1 n_1 + X_2 n_2 = 1$

$\Rightarrow$ bijection between $\mathbb{Z}_p \times \mathbb{Z}_q$

$n_1 = 3$, $n_2 = 5$ } $N = 15$

Example : $9 \bmod 15 \Rightarrow (0, 4)$

$\mathbb{Z}_{15} = \mathbb{Z}_3 \times \mathbb{Z}_5$ (x, y)

$7 \times 0 + 9 \times 4 = 36 \equiv 6 \bmod 15$ NO
$6 \times 0 + 10 \times 4 = 40 \equiv 10 \bmod 15$ NO

$10x + 6y = 24 \equiv 9 \bmod 15$

OPPURE ↔

$\mathbb{Z}_3^{(x)}$	$\mathbb{Z}_5^{(x)}$	$\mathbb{Z}_{15}$
0	0	0
1	1	1
2	2	2
0	3	3
1	4	4
2	0	5
0	1	6
1	2	7
2	3	8
0	4	9
1	0	10
2	1	11
0	2	12
1	3	13
2	4	14
0	0	15

Another method

$f(a,b) = a f(1,0) + b f(0,1)$ Linear Combination

$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 0 \bmod 5 \end{cases}$

If $x \equiv 0 \bmod 5$, then $x = 5y$

$5y \equiv 1 \bmod 3$

$\Rightarrow y = 5^{-1} \bmod 3 = 2$

$x = 5y = 10$

DSA Key generation

Alice generates a secret key $SK_A = 4$ and wants to generate a DS. Prime numbers $p = 11, q = 5$

What is the public key?

Solution: Key generation for DSA

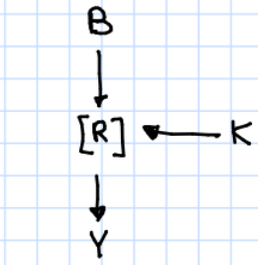
- generate a prime $p \Rightarrow p = 11$
- find a prime divisor q of $p-1$
  $p - 1 = 10 \Rightarrow q = 5$
- find an element α with $ord(\alpha) = q$, i.e α generates the subgroup with q elements

  $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \Rightarrow \alpha = 3 \quad 9 \cdot 9 \cdot 3 = 1 \bmod 11$

  $\alpha^q \equiv 1 \bmod q \Rightarrow 3^5 = 3^2 \cdot 3^3 = 9 \cdot 9 \cdot 3 = 1 \bmod 11$

- Choose a random integer d with $0 < d < q$
  $d = 4$
- Compute $\beta = \alpha^d \bmod p = 3^4 \bmod 11 = 9 \cdot 3 \cdot 3 = 4$

Feistel Scheme



B = 1100 1111

K = 1111

Y?

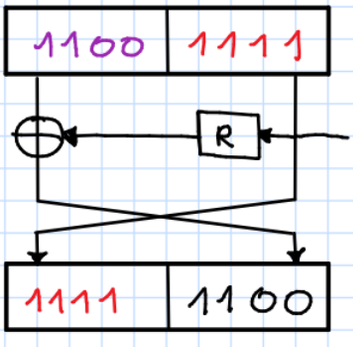
a) Y = 1111 1111

b) Y = 1100 1111

c) Y = 1111 1100 ✓

d) Y = 0000 0000

Solution: R is a XOR operation. The Feistel network works this way:



• DES Algorithm

Compute the value of $S_1(22)$ in DES algorithm

Here is S_1:

S_1	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

a) $S_1(22) = 14$

b) $S_1(22) = 11$

c) $S_1(22) = 12$ ✓

d) $S_1(22) = 7$

0 1 0 1 1 0

2^5 2^4 2^3 2^2 2^1 2^0

32 16 8 4 2 1

Solution

First of all we transform 22 in binary using 6 bit

$22|_{10} = 2^4 + 2^2 + 2^1 = 010110$

row = 0

col = 11

Compute the value of S(55)

$55 = 32+16+4+2+1 = 2^5+2^4+2^2+2^1+2^0 = 110111$

col 11

row 3

S(55) = 14

Binary Conversion

1 1 0 1 1 1

2^5 2^4 2^3 2^2 2^1 2^0

32 16 8 4 2 1

- DES Permutation

Here the tables of DES permutations IP and its inverse

ble 3.1 Initial permutation *IP*

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

Table 3.2 Final permutation IP^{-1}

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

Compute the first row of the table corresponding to the composition

$IP^2 = IP \circ IP$

Solution: in the first position we put the value "pointed" by the value of the first position of IP and so on

$IP(0,0) = 58$ => go to the 58^{th} position => 55

$IP^2(0,0) = 55$

...

55	53	51	49	56	54	52	50

• Addition Table

Let $E(\mathbb{Z}_{17})$ be the elliptic curve given by the equation $y^2 \equiv x^3 + 7$. Alice and Bob use $G(2,7)$ as generator for a ECDH to obtain a key session k.
Alice's secret key is $sk_A = 5$, Bob's secret key is $B = 12$. What of the following is the session key?

The following is the addition table on $E(\mathbb{Z}_{17})$ where ∞ is the neutral element.

·	∞	(1,5)	(1,12)	(2,7)	(2,10)	(3,0)	(5,8)	(5,9)	(6,6)	(6,11)	(8,3)	(8,14)	(10,2)	(10,15)	(12,1)	(12,16)	(15,4)	(15,13)
∞	∞	(1,5)	(1,12)	(2,7)	(2,10)	(3,0)	(5,8)	(5,9)	(6,6)	(6,11)	(8,3)	(8,14)	(10,2)	(10,15)	(12,1)	(12,16)	(15,4)	(15,13)
(1,5)	(1,5)	(2,10)	∞	(1,12)	(5,9)	(15,13)	(2,7)	(12,1)	(8,14)	(6,6)	(6,11)	(10,15)	(8,3)	(15,4)	(12,16)	(5,8)	(3,0)	(10,2)
(1,12)	(1,12)	∞	(2,7)	(5,8)	(1,5)	(15,4)	(12,16)	(2,10)	(6,11)	(8,3)	(10,2)	(6,6)	(15,13)	(8,14)	(5,9)	(12,1)	(10,15)	(3,0)
(2,7)	(2,7)	(1,12)	(5,8)	(12,16)	∞	(10,15)	(12,1)	(1,5)	(8,3)	(10,2)	(15,13)	(6,11)	(3,0)	(6,6)	(2,10)	(5,9)	(8,14)	(15,4)
(2,10)	(2,10)	(5,9)	(1,5)	∞	(12,1)	(10,2)	(1,12)	(12,16)	(10,15)	(8,14)	(6,6)	(15,4)	(6,11)	(3,0)	(5,8)	(2,7)	(15,13)	(8,3)
(3,0)	(3,0)	(15,13)	(15,4)	(10,15)	(10,2)	∞	(8,14)	(8,3)	(12,16)	(12,1)	(5,9)	(5,8)	(2,10)	(2,7)	(6,11)	(6,6)	(1,12)	(1,5)
(5,8)	(5,8)	(2,7)	(12,16)	(12,1)	(1,12)	(8,14)	(5,9)	∞	(10,2)	(15,13)	(3,0)	(8,3)	(15,4)	(6,11)	(1,5)	(2,10)	(6,6)	(10,15)
(5,9)	(5,9)	(12,1)	(2,10)	(1,5)	(12,16)	(8,3)	∞	(5,8)	(15,4)	(10,15)	(8,14)	(3,0)	(6,6)	(15,13)	(2,7)	(1,12)	(10,2)	(6,11)
(6,6)	(6,6)	(8,14)	(6,11)	(8,3)	(10,15)	(12,16)	(10,2)	(15,4)	(1,5)	∞	(1,12)	(2,10)	(2,7)	(5,9)	(3,0)	(15,13)	(12,1)	(5,8)
(6,11)	(6,11)	(6,6)	(8,3)	(10,2)	(8,14)	(12,1)	(15,13)	(10,15)	∞	(1,12)	(2,7)	(1,5)	(5,8)	(2,10)	(15,4)	(3,0)	(5,9)	(12,16)
(8,3)	(8,3)	(6,11)	(10,2)	(15,13)	(6,6)	(5,9)	(3,0)	(8,14)	(1,12)	(2,7)	(5,8)	∞	(12,16)	(1,5)	(10,15)	(15,4)	(2,10)	(12,1)
(8,14)	(8,14)	(10,15)	(6,6)	(6,11)	(15,4)	(5,8)	(8,3)	(3,0)	(2,10)	(1,5)	∞	(5,9)	(1,12)	(12,1)	(15,13)	(10,2)	(12,16)	(2,7)
(10,2)	(10,2)	(8,3)	(15,13)	(3,0)	(6,11)	(2,10)	(15,4)	(6,6)	(2,7)	(5,8)	(12,16)	(1,12)	(12,1)	∞	(8,14)	(10,15)	(1,5)	(5,9)
(10,15)	(10,15)	(15,4)	(8,14)	(6,6)	(3,0)	(2,7)	(6,11)	(15,13)	(5,9)	(2,10)	(1,5)	(12,1)	∞	(12,16)	(10,2)	(8,3)	(5,8)	(1,12)
(12,1)	(12,1)	(12,16)	(5,9)	(2,10)	(5,8)	(6,11)	(1,5)	(2,7)	(3,0)	(15,4)	(10,15)	(15,13)	(8,14)	(10,2)	(1,12)	∞	(8,3)	(6,6)
(12,16)	(12,16)	(5,8)	(12,1)	(5,9)	(2,7)	(6,6)	(2,10)	(1,12)	(15,13)	(3,0)	(15,4)	(10,2)	(10,15)	(8,3)	∞	(1,5)	(6,11)	(8,14)
(15,4)	(15,4)	(3,0)	(10,15)	(8,14)	(15,13)	(1,12)	(6,6)	(10,2)	(12,1)	(5,9)	(2,10)	(12,16)	(1,5)	(5,8)	(8,3)	(6,11)	(2,7)	∞
(15,13)	(15,13)	(10,2)	(3,0)	(15,4)	(8,3)	(1,5)	(10,15)	(6,11)	(5,8)	(12,16)	(12,1)	(2,7)	(5,9)	(1,12)	(6,6)	(8,14)	∞	(2,10)

(10,15)
(5,9) ✗
(6,6)
(5,8)

Protocol:

Alice		Bob
chooses sk 5		Chooses $sk_B = 12$
computes pk $5 \cdot G$	$\xleftarrow{PK_B}$	computes $pk_B = 12 \cdot G$
	$\xrightarrow{PK_A}$	
		$K = 12 \cdot PK_A$

$pK_A = 5G = 2G + 2G + G = (12,16) + (12,16) + (2,7) = (1,5) + (2,7) = (1,12)$

$pk_B = 12G = 5G + 5G + 2G = (1,12) + (1,12) + (12,16) = (2,7) + (12,16) = (5,9)$

$K = 12 pK_A = 12(1,12) = 6 \cdot 2(1,12) = 6 \cdot (2,7) = 2(2,7) + 2(2,7) + 2(2,7) = (12,16) + (12,16) + (12,16) =$

$= (1,5) + (12,16) = (5,8)$

• Linear PRNG

Seed $S_0 = 2$

$S_1, S_2 \ldots$ numbers generated by a Linear PRNG with $a = 5, b = 1 \bmod 23$

$S_2 = ?$

a) 6

b) 17

c) 15

d) 10 ✓

e) 13

> **Pseudo Random Number Generator**
>
> $S_0 =$ seed
>
> $S_{i+1} = a\,S_i + b \pmod n$

Solution:

$S_0 = \text{seed}$

$S_{i+1} = aS_i + b \bmod n$

$S_1 = aS_0 + b \bmod n = 5 \cdot 2 + 1 \bmod 23 = 11$

$S_2 = aS_1 + b \bmod n = 5 \cdot 11 + 1 = 10$

- **Esercizio doppia cifratura** NEW!

Let $Enc^1_k(P) = k \oplus P$ be the Vernam or XOR cipher of 3-bit blocks

Let $Enc^2_k(P) = k \boxtimes P$ be the moltiplication chiper modulo $8 = 2^3$ where k, P are the binary expression of elements of $\mathbb{Z}_8$

Let $Enc_k(P) = Enc^2_{k_2}(Enc^1_{k_1}(P))$ be the 3-bit double-encryption

Knowing that $Enc_k(3) = 4$ $\quad Enc_k(4) = 7$

$$\begin{cases} k_2 \boxtimes (3 \oplus k_1) = 4 \mod 8 \\ k_2 \boxtimes (3 \oplus k_1) = 7 \mod 8 \end{cases}$$

$$\begin{cases} k_2 \boxtimes 3 \oplus k_2 \boxtimes k_1 = 4 \mod 8 \\ k_2 \boxtimes 4 \oplus k_2 \boxtimes k_1 = 7 \mod 8 \end{cases}$$

$$\begin{cases} k_2 \boxtimes k_1 = k_2 \boxtimes 3 \oplus 4 \mod 8 \\ k_2 \boxtimes k_1 = k_2 \boxtimes 4 \oplus 7 \mod 8 \end{cases} \Rightarrow 4 \oplus 3 \boxtimes k_2 = 7 \oplus 4 \boxtimes k_2$$

$$\Rightarrow \underbrace{7 \oplus 4}_{3} \oplus 3 \boxtimes k_2 = 4 \boxtimes k_2 \Rightarrow 3 \oplus 3 \boxtimes k_2 = 4 \boxtimes k_2$$

$$\Rightarrow 3 + 3 \boxtimes k_2 + 4 \boxtimes k_2 = 0 \Rightarrow 3 + \underbrace{(3+4)}_{7} \boxtimes k_2 = 0$$

$$\Rightarrow 7 \boxtimes k_2 = 3 \Rightarrow k_2 = 3 \boxtimes 7^{-1}$$

↳ euclide $7^{-1} \bmod 8 = 7$

$$\Rightarrow k_2 = 3 \boxtimes 7 \Rightarrow k_2 = 21 \mod 8 \Rightarrow k_2 = 5$$

$$(3 \oplus k_1) \boxtimes k_2 = 4 \Rightarrow (3 \oplus k_1) \boxtimes 5 = 4$$

$$\Rightarrow \underbrace{3 \boxtimes 5}_{15 \bmod 8} \oplus 5 \boxtimes k_1 = 4 \Rightarrow 7 \oplus 5 \boxtimes k_1 = 4$$

$\Rightarrow$ $5 \boxtimes K_1 = \underbrace{4 \oplus 7}_{3}$ $\Rightarrow$ $K_1 = 3 \boxtimes 5^{-1}$

↳ euclide $5^{-1} \bmod 8 = 5$

$\Rightarrow$ $K_1 = 3 \boxtimes 5 = 7 \bmod 8$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$1 = 3 - 2$

$1 = 3 - (5 - 3)$

$1 = 3 - 5 + 3$

$1 = 3 \times 2 - 5$

$1 = (8 - 5) \times 2 - 5$

$1 = 8 \times 2 - 3 \times 5$

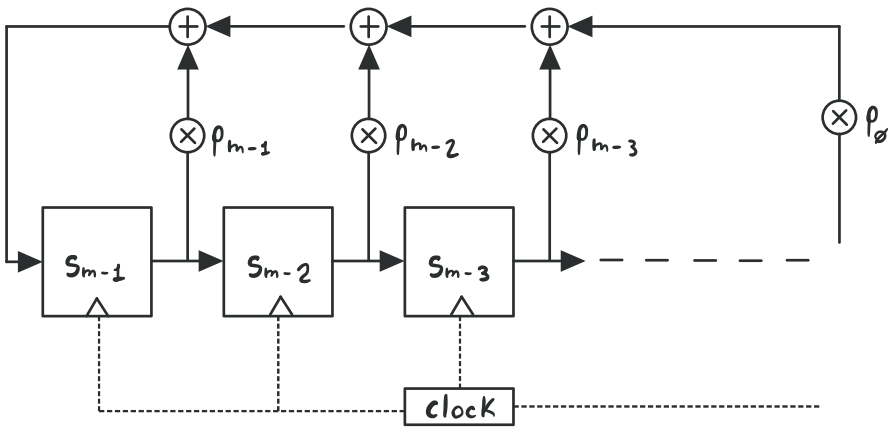
$-3 \bmod 8$

5

$(K_1, K_2) = (7, 5)$ ✓

- LFSR

Compute the bits S_5, S_4, S_3, S_2 of the stream generated by the Fibonacci LFSR whose polynomial is $\chi_L(x) = x^2 + x + 1$ and the first bits are $s_0 = 0$, $s_1 = 1$



numero FF = grado funzione = (2 in questo caso)

XOR	s_1	s_0		R(shift)	
1	1	0			Init
0	1	1	$\Rightarrow$	0	s_0
1	0	1	$\Rightarrow$	1	s_1
1	1	0	$\Rightarrow$	1	s_2
0	1	1	$\Rightarrow$	0	s_3
1	0	1	$\Rightarrow$	1	s_4
1	1	0	$\Rightarrow$	1	s_5

Es: CRT System

$$\begin{cases} X \equiv 4 \bmod 11 \\ X \equiv 3 \bmod 17 \\ X \equiv 6 \bmod 18 \end{cases}$$

$N = 3366 = 11 \cdot 17 \cdot 18$

$b_1 = 4 \; ; N_1 = 306 \to N/11$
$b_2 = 3 \; ; N_2 = 198 \to N/17$
$b_3 = 6 \; ; N_3 = 187 \to N/18$

b_i	N_i	x_i	$b_i N_i x_i$
4	306	5	6120
3	198	14	8316
6	187	13	14586

$X_1 = 306^{-1} \bmod 11$

$306 \equiv 9 \bmod 11 \Rightarrow 9^{-1}$

$306x \equiv 1 \bmod 11$
$9x \equiv 1 \bmod 11$

$11 = 9 \times 1 + 2$
$9 = 2 \times 4 + 1$
$4 = 1 \times 4 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 2 \bmod 11 = 10$
$p_3 = 1 - 10 \times 4 \bmod 11 \equiv 5$

$198 \equiv 11 \bmod 17$
$17 = 11 \times 1 + 6$
$11 = 6 \times 1 + 5$
$6 = 5 \times 1 + 1$
$5 = 1 \times 5 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 1 \bmod 17 = 16$
$p_3 = 1 - 16 = 2$
$p_4 = 16 - 2 = 14$

$187 \equiv 7 \bmod 18$

$18 = 7 \times 2 + 4$
$7 = 4 \times 1 + 3$
$4 = 3 \times 1 + 1$
$3 = 1 \times 3 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 2 = 16$
$p_3 = 1 - 16 = 3$
$p_3 = 16 - 3 = 13$

$$X = 6120 + 8316 + 14586 = 2754 + 1584 + 1122 \equiv 2094 \bmod 3366$$

SCHEMA A SOGLIA SHAMIR

Supponiamo di avere a disposizione le prime m ombre: (x_1, y_1), (x_2, y_2) $\ldots (x_m, y_m)$. Poiché il polinomio $F(x)$ ha m coefficienti e grado $m-1$, la conoscenza delle prime m ombre consente di scrivere il sistema lineare :

$M + a_1 x_1 + a_2 x_1^2 + \ldots a_{m-1} x_1^{m-1} = y_1$ $M + a_1 x_2 + a_2 x_2^2 + \ldots a_{m-1} x_2^{m-1} = y_2$

$\ldots$

$M + a_1 x_m + a_2 x_m^2 + \ldots a_{m-1} x_m^{m-1} = y_m$

(sistema in $\mathbb{Z}_p$) dove le ombre (x_i, y_i) sono i dati noti e le incognite sono invece i valori $\{M, a_1, a_2, \ldots, a_{m-1}\}$.

$\mathbb{Z}_p$

$A = (x_A, y_A)$ $B = (x_B, y_B)$ $C = (x_C, y_C)$ NOTI

polinomio di grado $m-1$ $F(x) = M + a_1 x + a_2 x^2$ mod p

$$\Rightarrow \begin{cases} y_A = M + a_1 x_A + a_2 x_A^2 \\ y_B = M + a_1 x_B + a_2 x_B^2 \\ y_C = M + a_1 x_C + a_2 x_C^2 \end{cases} \rightarrow$$

Le incognite sono 3

M, a_1, a_2

oppure $F(x) = \sum_{j=1}^{k} p_j(x)$; $p_j(x) = y_j \prod_{\substack{m=1 \\ m \neq j}}^{k} \frac{x - x_m}{x_j - x_m}$

x 3 punti

$$F(x) = y_1 \left(\frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} \right) + y_2 \left(\frac{x - x_1}{x_2 - x_1} \cdot \frac{x - x_3}{x_2 - x_3} \right) + y_3 \left(\frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_2}{x_3 - x_2} \right)$$

$$P(x) = y_1 \left(\frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} \right) + y_2 \left(\frac{x - x_1}{x_2 - x_1} \cdot \frac{x - 3}{x_2 - x_3} \right) + y_3 \left(\frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_2}{x_3 - x_2} \right)$$

$$P(x) = 1716 \left(\frac{x - 27}{18 - 27} \cdot \frac{x - 31}{18 - 31} \right) + 3768 \left(\frac{x - 18}{27 - 18} \cdot \frac{x - 31}{27 - 31} \right) + 4940 \left(\frac{x - 18}{31 - 18} \cdot \frac{x - 27}{31 - 27} \right)$$

$$P(x) = 42 + 3x + 5x^2$$