SOLUTION OF THE EQUATION

- let $p=11 \quad q=19 \quad n=p \cdot q=209$

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

PROCEDURE

① Use CRT $\rightarrow$ $209 = 11 \times 19$ $\rightarrow$ We decompose the equation into two sub equations w smaller mod

$$x^2 \equiv 171 \bmod 11 = 6 \bmod 11$$
$$x^2 \equiv 171 \bmod 19 = 0 \bmod 19$$

② Check that the solutions are quadratic residue:

0 can be ignored

$6^{\frac{11-1}{2}} \equiv 1 \bmod 11 \rightarrow 6^5 \equiv 10 \bmod 11 \rightarrow$ NOT A QUADRATIC RESIDUE

$\Rightarrow$ THIS IMPLIES NO SOLUTION

a. 1
b. 3
c. $\emptyset$ ✓ $\rightarrow$ There are no solutions
d. 4
e. 2

- let $p=11 \quad q=19 \quad pq=209$ How many solutions does $x^2 \equiv 130 \bmod 209$ have?

① $\begin{cases} x^2 \equiv 130 \bmod 11 = 9 \bmod 11 \\ x^2 \equiv 130 \bmod 19 = 16 \bmod 19 \end{cases}$

② $x \equiv \pm 3 \bmod 11$
$x \equiv \pm 4 \bmod 19$ → THE ARE SOLUTIONS ONLY IF THEY ARE QUADRATIC RESIDUE

TO CHECK IF THEY ARE QUADRATIC RESIDUE:

$p=11, q=19$

$9^{\frac{11-1}{2}} \equiv 1 \bmod 11$?

$9^5 \equiv 9^2 \cdot 9^2 \cdot 9 \bmod 11$
$\equiv 4 \cdot 4 \cdot 9 \bmod 11$
$\equiv 16 \cdot 9 \bmod 11$
$\equiv 5 \cdot 9 \bmod 11$
$\equiv 45 \bmod 11$
$\equiv 1 \bmod 11$

$16^{\frac{19-1}{2}} \equiv 1 \bmod 19$?

$16^9 \equiv 16^2 \cdot 16^2 \cdot 16^2 \cdot 16^2 \cdot 16 \bmod 19$
$\equiv 9 \cdot 9 \cdot 9 \cdot 9 \cdot 16 \bmod 19$
$\equiv 9^2 \cdot 9^2 \cdot 16 \bmod 19$
$\equiv 5 \cdot 5 \cdot 16 \bmod 19$
$\equiv 6 \cdot 16 \bmod 19$
$\equiv 1 \bmod 19$

since they are both 1 they are quadratic residue and so the equation has 4 solutions

a. 1
b. 4 ✓
c. 2
d. 3
e. ∅

- FROM TELEGRAM

$17x \equiv 1 \bmod 29$

$x \equiv 1 \cdot 17^{-1} \bmod 29$

$29 = 1 \cdot 17 + 7$
$17 = 2 \cdot 7 + 3$
$7 = 2 \cdot 3 + 1$

$1 = 7 - 2 \cdot 3$
$1 = 7 - 2(17 - 2 \cdot 7)$
$\overset{!}{=} 7 - 2 \cdot 17 + 4 \cdot 7 = 5 \cdot 7 - 2 \cdot 17$

$1 = 5 \cdot (29 - 1 \cdot 17) - 2 \cdot 17$
$\overset{!}{=} 5 \cdot 29 - 5 \cdot 17 - 2 \cdot 17$
$\overset{!}{=} 5 \cdot 29 - 7 \cdot 17$
↑

-7 in $\bmod 29 \rightarrow 17$

• FROM TELEGRAM 2

find the solutions of $x^2 \equiv 1 \bmod 24$

PROCEDURE:

use the CRT to split the equation $\begin{cases} x^2 \equiv 1 \bmod 8 \rightarrow 1^{\frac{8-1}{2}} \equiv 1 \bmod 8 \checkmark \\ x^2 \equiv 1 \bmod 3 \rightarrow 1^{\frac{3-1}{2}} \equiv 1 \bmod 3 \checkmark \end{cases}$

we have to find the values of x^2 w mod 8 and mod 3

① find all x w $[0,7]$

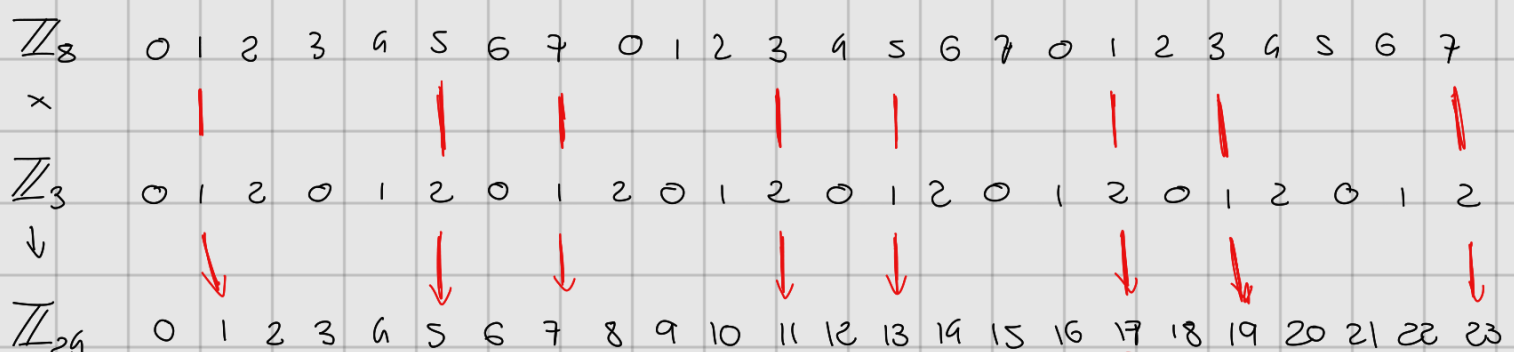
$0^2 \equiv 1 \bmod 8$ ✗
$1^2 \equiv 1 \bmod 8$ ✓
$2^2 \equiv 1 \bmod 8$ ✗
$3^2 \equiv 1 \bmod 8$ ✓
$4^2 \equiv 1 \bmod 8$ ✗
$5^2 \equiv 1 \bmod 8$ ✓
$6^2 \equiv 1 \bmod 8$ ✗
$7^2 \equiv 1 \bmod 8$ ✓

② find all x in $[0,2]$

$0^2 \equiv 1 \bmod 3$ ✗
$1^2 \equiv 1 \bmod 3$ ✓
$2^2 \equiv 1 \bmod 3$ ✓

The solutions are:
① → 1, 3, 5, 7
② → 1, 2

Construct them back with CRT



Solution of the original equation: 1, 5, 7, 11, 13, 17, 19, 23

MAPPING AND ISOMORPHISM

2022-06-27

- Let $f: \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$ 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. $f(x,y) = 12x + 4y$

PROCEDURE (SMART WAY)

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

$$f(x,y) = af(1,0) + bf(0,1)$$

$$= 10x + 6y$$

- Let $f: \mathbb{Z}_5 \times \mathbb{Z}_7 \to \mathbb{Z}_{35}$ be the isomorphism of the CRT

a. $f(x,y) = 20x + 16y$
b. $f(x,y) = 21x + 15y$ ✓
c. $f(x,y) = 15x + 21y$
d. $f(x,y) = 17x + 19y$

PROCEDURE (BRUTE FORCE)

$\mathbb{Z}_5$	$\mathbb{Z}_7$	$\mathbb{Z}_{35}$
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
0	5	5 →
1	6	6 →
2	0	7
3	1	8
4	2	9
⋮	⋮	⋮

PLUG IN ⇒ $21(0) + 15(5) = 75$, $21(1) + 15(6) = 111$

$75 = 5 \bmod 35$ ✓
$111 = 6 \bmod 35$ ✓

Continue but not important

2021_07_16

- let $f: \mathbb{Z}_4 \times \mathbb{Z}_5 \to \mathbb{Z}_{20}$ be the isomorphism of CRT,

a. $f(x,y) = 16x + 5y$
b. $f(x,y) = 13x + 8y$
c. $f(x,y) = 5x + 16y$ ✓
d. $f(x,y) = 8x + 13y$

0	0	0
1	1	1
2	2	2
3	3	3
0	4	4
(1	0) →	5
2	1	6
3	2	7
0	3	8
1	4	9
2	0	10
3	1	11
0	2	12
1	3	13
2	4	14
3	0	15
(0	1) →	16
1	2	17
2	3	18
3	4	19
⋮	⋮	
1	⋮	

$$f(x,y) = ax + by$$

as we can see from the answares the funcion $f(x,y)$ is composed of a linear combination of 2 independent variable

The x component is given by the eigenvector which is $f(1,0)$ and y component from $f(0,1)$. We have to find it in the CR

$$f(x,y) = 5x + 16y$$

DSA exercises

- We need p large enough ($2^{1023} < p < 2^{1024}$) and q which is a prime divisor of $p-1$. Usually p and q are given in the exercises

- Find an element α such that $ord(\alpha) = q$ i.e. α generates the entire subgroup with q elements.
  Calculating the order of an element means finding out to which number I have to raise α to get the identity in that set.

  $\alpha^n \equiv 1 \bmod p$ where $\mathbb{Z}_p$ is the set and n is the order of an element

FOR THE EXERCISES:

we need to find an element that has $ord(\alpha) = q$, so we can try directly test the elements of the set for this condition. Specifically we can always test that $\alpha^q \equiv 1 \bmod p$, we use q as exponent because we want to test specifically the condition of $ord(\alpha) = q$.

Given p, q and α we still have to find $\beta = \alpha^d \bmod p$
d is generally given and should be $0 < d < q$

The element (p, q, α, β) represents the pk

- 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?

PROCEDURE

① Generate a prime and a prime divisor (already given)

$p = 11 \rightarrow p - 1 = 10 \rightarrow q = 5$

② Find an element α with $ord(\alpha) = q$, i.e. generate the subgroup with a q elements $\mathbb{Z}_5^* = \{\cancel{0}, 1, 2, 3, 4\}$

$\alpha = 3 \quad \alpha^q \equiv 1 \bmod q \rightarrow 3^5 \equiv 1 \bmod 5$

$3^2 \cdot 3^2 \cdot 3 \Rightarrow 9 \cdot 9 \cdot 3$

$4 \cdot 4 \cdot 3 = 16 \cdot 3$

2021_09_14

- DSA algorithm. Given $p=11$ $q=5$ $d=9$, what is the public key?

a. $(11, 5, 9, 5)$

b. $(11, 5, 3, 5)$

c. $(11, 5, 7, 3)$

d. $(11, 5, 2, 9)$

e. $(11, 5, 4, 2)$

PROCEDURE:

The last 2 elements of each row must be analyzed

Remember that we have to find a generator $\alpha \in \mathbb{Z}_p$

with $\text{ord}(\alpha) = q$ ie. an element which generates $\mathbb{Z}_q$

such that $\alpha^q \equiv 1 \bmod p$

FROM ANSWARES ↓

We have that the possible values of α are $\{9, 3, 7, 2, 9\}$

we try all options and see which α generates the

entire set

a. $9 \Rightarrow 9^5 \equiv 1 \bmod 11$?

9 base element, res = 1, 5 = 101

FROM LSB TO MSB

- 1 → $1 \cdot 1 \bmod 11 = 1$
  $1 \cdot 9 \bmod 11 = 9$
- 0 → $9 \cdot 9 \bmod 11 = 4$
- 1 → $4 \cdot 4 \bmod 11 = 5$
  $5 \cdot 9 \bmod 11 = 1$

THIS MEANS THAT $9^5 \equiv 1 \bmod 11$ ✓

b. $3 \Rightarrow 3^5 \equiv 1 \bmod 11$?

$3^3 \cdot 3^2 = 5 \cdot 9 \bmod 11 = 45 \bmod 11 \equiv 1 \bmod 11$ ✓

c. $7 \Rightarrow 7^5 \equiv 1 \bmod 11$?

$7^2 \cdot 7^2 \cdot 7 = 5 \cdot 5 \cdot 7 = 25 \cdot 7 = 3 \cdot 7 \bmod 11 = 10$ ✗

d. $2 \Rightarrow 2^5 \equiv 1 \bmod 11$?

$32 = 10 \bmod 11$ ✗

e. $4 \Rightarrow 4^5 \equiv 1 \bmod 11$

$4^2 \cdot 4^2 \cdot 4 = 5 \cdot 5 \cdot 4 \bmod 11 = 3 \cdot 4 \equiv 1 \bmod 11$ ✓

So now we have 3 possible candidates: $\{9, 3, 4\}$

and we have to check the last value

$\beta = \alpha^d \bmod p \rightarrow \beta_1 = 9^4 \bmod 11 = 5$ ✓

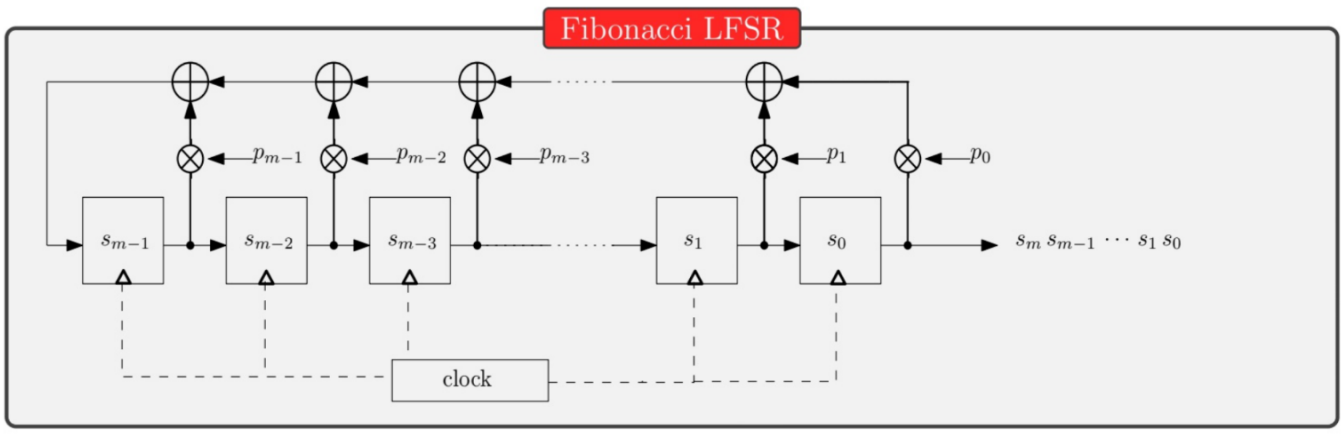
$\beta_2 = 3^4 \bmod 11 = 4$

$\beta_3 = 4^4 \bmod 11 = 3$

THE ONLY OPTION THAT MATCHES IS OPTION (A)

FIBONACCI LFSR

2.4.1 Fibonacci LFSRs



The output bit s_m is computed as a feedback

$$s_m = f(\mathbf{s}) = \sum_{j=0}^{m-1} s_j \cdot p_j$$

The feedback polynomial is : $P(x) = 1 + p_{m-1}x + \cdots + p_1 x^{m-1} + p_0 x^m$ and the characteristical polynomial is

$$\chi_{\mathrm{L}}(x) = x^m P(\frac{1}{x}) = p_0 + p_1 x + \cdots + p_{m-1}x^{m-1} + x^m \ .$$

Here the involved linear map L is:

$$\mathrm{L} = \begin{bmatrix} p_{m-1} & 1 & 0 & 0 & \cdots & 0 \\ p_{m-2} & 0 & 1 & 0 & \cdots & 0 \\ p_{m-3} & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_1 & 0 & 0 & 0 & \cdots & 1 \\ p_0 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

Being the state $\mathbf{s} = [s_{m-1}s_{m-2}s_{m-3}\cdots s_1 s_0]$ the transition to the state $\mathbf{s}'$ is given by the multiplication:

$$\mathbf{s} \cdot \mathrm{L} = \mathbf{s}' \,,$$

or at a bits level:

$$\mathbf{s}' = [f(\mathbf{s}) s_{m-1}s_{m-2}s_{m-3}\cdots s_2 s_1] \,.$$

2021_07_16

- An n-bit Fibonacci LFSR has n flip flops and produces an output stream $\ldots s_2 s_1 s_0$
If a sequence like ...01100001001... is detected in the output sheam, then:

a. m=4
b. m=2
c. m=5
d. m=3

The longest sequence of number is 4 zeros, m indicates the the number of flip flops. If the LFSR had 4 flip flops then the sheam would have been full of zeros from that point on. So m=5

from the slides

- This is a brute force attack against an LFSR (KPA)

We have a 3 bit LFSR and we have sniffed the sequence ...01110...
which means:

S_5	S_4	S_3	S_2	S_1	S_0
0	1	1	1	0	1

If we want to attack an n bit LFSR we need 2n S values

we can set up the following system

$$S_3 = S_2P_2 + S_1P_1 + S_0P_0$$
$$S_4 = S_3P_2 + S_2P_1 + S_1P_0$$
$$S_5 = S_4P_2 + S_3P_1 + S_2P_0$$

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} P_2 \\ P_1 \\ P_0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{array}{cccc} 1 & 0 & 1 & = 1 \\ 1 & 1 & 0 & = 1 \\ 0 & 1 & 0 & = 1 \end{array} \rightarrow \begin{array}{cccc} 1 & 0 & 1 & = 1 \\ 1 & 0 & 0 & = 0 \\ 0 & 1 & 0 & = 1 \end{array} \Rightarrow \begin{array}{l} P_1 = 1 \\ P_2 = 0 \\ P_1 = 1 \end{array} \rightarrow \begin{array}{l} P_2 = 0 \\ P_1 = 1 \\ P_0 = 1 \end{array}$$

ELLIPTIC CURVE

2021_07_02

- Let $E: y^2 \equiv x^3 + 2x + 2 \bmod 17$ an elliptic curve and let $P = (5,1)$ and $Q = (6,3)$ and $R = (x,y)$ such that $P + Q + R = \emptyset$ Then R is:

PROCEDURE

$P + Q + R = \emptyset \rightarrow P + Q = -R$

Point of negation $\rightarrow$ if $R(x_3, y_3)$ then $-R(x_3, -y_3)$

$P(x_1, y_2) + Q(x_2, y_2) = -R(x_3, -y_3)$

I can define $-R$ as R^*

The x coordinates of $R = P + Q$ is given by:

$$xR = m^2 - x_1 - x_2$$

The y coordinates of $R = P + Q$ is given by:

$$yR = m * (x_1 - xR) - y_1$$

Then $m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3-1}{6-5} = 2 \equiv 2 \bmod 17$

$xR = 4 - 5 - 6 = -7 \equiv 10 \bmod 17$

$yR = 2 * (5 - 10) - 1 = -10 - 1 = -11 \equiv 6 \bmod 17$

$R^* = (10, 6) \rightarrow R = (10, -6) = (10, 11)$

2021_07_02

- Let $E: y^2 \equiv x^3 + 2x + 2 \mod 17$ an elliptic curve and let $P = (6,3)$ and $Q = (10,6)$ and $R = (x,y)$ such that $P + Q + R = 0$

PROCEDURE:

$$P + Q = -R \rightarrow R = (x_3, y_3) \quad -R(x_3, -y_3) \Rightarrow R^* = -R$$

$$\Rightarrow P + Q = R^*$$

$$m = (y_2 - y_1)/(x_2 - x_1) = \frac{6-3}{10-6} = \frac{3}{4} = 3 \cdot 4^{-1} \mod 17$$

we have to find $4^{-1} \rightarrow 4 \cdot b \equiv 1 \mod 17$ we have to find b

Since the numbers are small we can brute force it:

$4 \cdot 4 \rightarrow 16$
$5 \rightarrow 20 \rightarrow 3 \mod 17$
$6 \rightarrow 24 \rightarrow 8 \mod 17$
$7 \rightarrow 28 \rightarrow 12 \mod 17$
$8 \rightarrow 32 \rightarrow 16 \mod 17$
$9 \rightarrow 36 \rightarrow 2 \mod 17$
$10 \rightarrow 40 \rightarrow 6 \mod 17$
$11 \rightarrow 44 \rightarrow 10 \mod 17$
$12 \rightarrow 48 \rightarrow 14 \mod 17$
$13 \rightarrow 52 \rightarrow 1 \mod 17 \Rightarrow$ FOUND IT $\Rightarrow 4 \cdot 13 \equiv 1 \mod 17$

$$m = 3 \cdot 13 \mod 17 \equiv 39 \mod 17 \equiv 5 \mod 17$$

$$x_R = m^2 - x_1 - x_2 = 25 - 6 - 10 \equiv 9 \bmod 17$$

$$y_R = m \cdot (x_1 - x_R) - y_1 = 5 \cdot (6-9) - 3 \equiv -18 \bmod 17$$
$$\equiv 16 \bmod 17$$

$$R^* = (9, 16) \Rightarrow R = (9, -16) = (9, 1)$$

NOTE: $-18 \bmod 17 \rightarrow$

$$\begin{array}{r|l} -18 & 17 \\ \hline 17 & 1 \\ \hline -1 & \end{array}$$

-1 is the result but we usually want them to be positive so we could the $17 \rightarrow +16$

$$\begin{array}{r|l} -16 & 17 \\ \hline 0 & 0 \\ \hline -16 & \end{array}$$

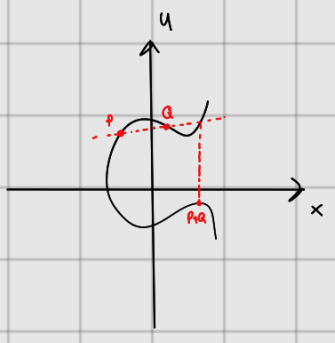
$-16 + 17 = 1$

2022_06_27

- Let $E: y^2 \equiv x^3 + 2x + 3 \bmod 17$ an elliptic curve and let $P = (5,1)$ such that $P+Q+R = \emptyset$ what is R?

$P+Q = -R \rightarrow R = (x,y) \Rightarrow -R = (x,-y)$ $\quad R^* = -R$

$P+Q = R^*$



first find m $\rightarrow m = \frac{3-1}{6-1} = 2$

$R^* = (x_R, y_R) \rightarrow x_R = m^2 - x_1 - x_2 = 4 - 5 - 6 = -7 \equiv 10 \bmod 17$

$y_R = m \times (m_1 - x_R) - y_1 = -11 \equiv 6 \bmod 17$

$R^* = (10,6) \rightarrow R = (10,-6) = (10,11)$

MULTIPLICATIVE INVERSE

2021_07_02

- Let $GF(8)$ be the Galois field defined by the polynomial

$$G(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$$

Let $a(x) \in GF(8)$ be $a(x) = x+1$. The multiplicative inverse of $a(x)$ is:

PROCEDURE:

Recall that $GF(8) \rightarrow GF(2^3)$ $\Rightarrow$ It has 8 elements and the multiplicative inverse must be among them

The multiplicative inverse is such that $a(x) \cdot a^{-1}(x) \equiv 1 \bmod G(x)$

①

$$\begin{array}{l|l} x^3 + 0x^2 + x + 1 & x+1 \\ \hline x^3 + x^2 & x^2 + x \\ \hline x^2 + x + 1 & \\ \hline x^2 + x & \\ \hline 1 & \end{array}$$

↑ This is the multiplicative inverse

→ I obtained 1

2021_07_02

- Let GF(8) be the Galois Field defined by the polynomial $G(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$

Let $a(x) \in GF(8)$ be $a(x) = x^2 + x$, the multiplicative inverse of $a(x)$ is:

$$\begin{array}{r|l} x^3 + 0x^2 + x + 1 & x^2 + x \\ \hline x^3 + x^2 & x + 1 \\ \hline x^2 + x + 1 & \\ x^2 + x & \\ \hline 1 & \end{array}$$

← This is the multiplicative inv.

→ Since I have obtained one

ANOTHER APPROACH → BRUTE FORCE

find among the answares the one for which:

$$a(x) \cdot a^{-1}(x) \equiv 1 \bmod G(x)$$

$$(x+1)(x^2+x) = x^3 + x^2 + x^2 + x = x^3 + x$$

$$
\begin{array}{l|l}
x^3+0x^2+x+0 & x^3+x+1 \\
\cancel{x^3+0+x+1} & \\
\hline
1 & 1
\end{array}
$$

This is 1 $\Rightarrow (x+1)(x^2+x) \equiv 1 \bmod G(\lambda)$

SYSTEM OF EQUATIONS IN MODULUS

2021_07_02

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

$$\begin{cases} x \cdot 56 \equiv 1 \bmod 401 \\ 5 \cdot x \equiv 308 \bmod 401 \end{cases}$$

We have to find x such that $56 \cdot x \equiv 1 \bmod 401$

which means that x is the inverse of 56. We can find it

with the extended euclidean algorithm:

① Apply EEA to find the GCD(56,401) untill remainder is $\emptyset$

$$401 = 7 \cdot 56 + 9$$

$$56 = 6 \cdot 9 + 2$$

$$9 = 4 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

② Work back words starting from the first non zero remainder

$9 = 4 \cdot 2 + 1 \quad \rightarrow \quad 1 = 9 - 4 \cdot 2$

Now substitute at each iteration:

$1 = 9 - 4 \cdot 2$

$1 = 9 - 4(56 - 6 \cdot 9) = -4 \cdot 56 + 25 \cdot 9$

$1 = -4 \cdot 56 + 25 \cdot (401 - 7 \cdot 56)$

$1 = -4x + 25 \cdot (9 - 7x)$

$= -4x + 25y - 175x$

$= -179 \cdot 56 + 25 \cdot 401$

↑ THIS IS THE INVERSE → $-179 + 401 = 222$

Try $5 \cdot 222 \equiv 308 \bmod 401$ ✓

2021_07_02

- Find $x \in 401$ such that

$$\begin{cases} x \cdot 29 \equiv 1 \bmod 401 \\ 5 \cdot x \equiv 14 \bmod 401 \end{cases}$$

OPTION 1

EEA: $x \cdot 29 \equiv 1 \bmod 401$

The inverse exists only if the $\gcd(29, 401) = 1$

$$401 = 29 \times 13 + 29$$

$$29 = 1 \cdot 29 + 5$$

$$29 = 4 \cdot 5 + 4$$

$$5 = 1 \cdot 4 + 1 \quad \rightarrow \text{START FROM THIS}$$

$$4 = 4 \cdot 1 + 0$$

$$1 = 5 - 1 \cdot 4$$

$$1 = 5 - 1 \cdot (29 - 4 \cdot 5) = -29 + 5 \cdot 5$$

$$1 = -29 + 5 \cdot (29 - 1 \cdot 29) = +5 \cdot 29 - 6 \cdot 29$$

$$1 = 5 \cdot 29 - 6(401 - 29 \cdot 13) = \underline{83} \cdot 29 - 6 \cdot 401$$

↓ continue

↑ INVERSE

OPTION 2

The shortest way could be to start from the second equation

$X \cdot 5 = 19 \bmod 401 \rightarrow X = 19 \cdot 5^{-1} \bmod 401$

we need to find 5^{-1} in 401 with EEA ↓

$$401 = 80 \cdot 5 + 1 \Rightarrow 1 = 401 - 80 \cdot 5$$

ONLY ONE STEP

-80 is the inverse $\Rightarrow -80 + 401 = 321$

$X = 19 \cdot 321 \bmod 401 = 83$

FROM THE SLIDES

find x such that $\begin{cases} x = 2 \bmod 3 \\ x = 3 \bmod 5 \\ x = 2 \bmod 7 \end{cases}$

from CRT we know that there exists an $N = 3 \cdot 5 \cdot 7 = 105$

we can transform the system such that:

$\begin{cases} Ax = 2 \bmod 3 \\ Bx = 3 \bmod 5 \\ Cx = 2 \bmod 7 \end{cases}$ $A = \frac{N}{3}$ $B = \frac{N}{5}$ $C = \frac{N}{7}$

$A = 35$ $B = 21$ $C = 15$

$\begin{cases} 35x = 2 \bmod 3 \\ 21x = 3 \bmod 5 \\ 15x = 2 \bmod 7 \end{cases}$ $\begin{cases} x = 2 \cdot 35^{-1} \bmod 3 \quad (1) \\ x = 3 \cdot 21^{-1} \bmod 5 \quad (2) \\ x = 2 \cdot 15^{-1} \bmod 7 \quad (3) \end{cases}$

(1) $3 = 35 \cdot 0 + 3$

$35 = 11 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$1 = 3 - 1 \cdot 2$

$1 = 3 - (35 - 3 \cdot 11) \cdot 1$

$\overset{!}{=} 3 - 35 + 11 \cdot 3 = 12 \cdot 3 - 35$

$35^{-1} \rightarrow -1 \Rightarrow$ in mod 3 $\Rightarrow +2$

$x = 2 \cdot 2 \bmod 3 = 1$

(2) $5 = 21 \cdot 0 + 5$

$21 = 4 \cdot 5 + 1$

$5 = 5 \cdot 1 + 0$

$1 = 21 - 4 \cdot 5$

$21^{-1} \rightarrow -4 \Rightarrow$ in mod 5 $\Rightarrow +1$

$x = 3 \cdot 1 \bmod 5 = 3$

(3) $7 = 15 \cdot 0 + 7$ $\quad 1 = 15 - 2 \cdot 7$

$15 = 2 \cdot 7 + 1$

$15^{-1} \to +1 \Rightarrow \text{in mod } 7 \Rightarrow +1$

$x = 2 \cdot 1 \bmod 7 = 2$

$x_1 = 1 \quad x_2 = 3 \quad x_3 = 2$

$x = 1 \cdot 35 + 3 \cdot 21 + 2 \cdot 15 \bmod 105$

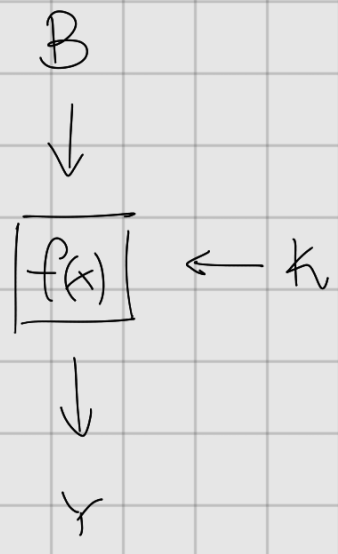
$= 70 + 63 + 30 \bmod 105$

$= 23$

FEISTEL SCHEMA

2021_09_19

- Consider the following Feistel scheme

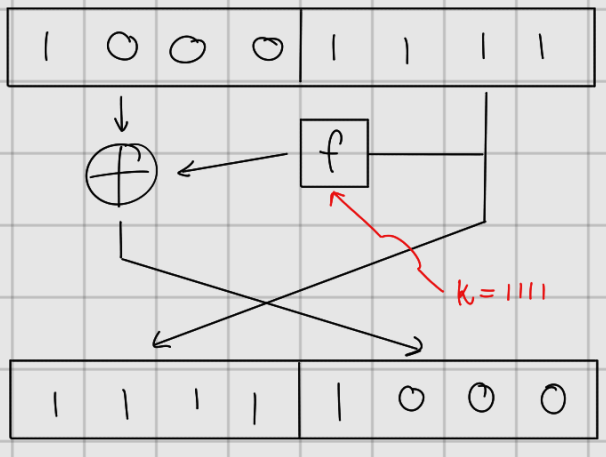


$B = 1000\ 1111$

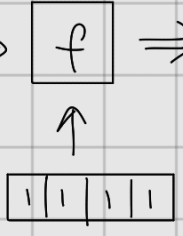
$k = 1111$

$f(x) = x \oplus k$

Solution :

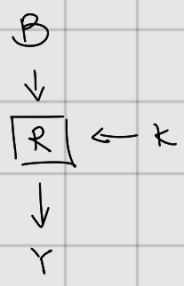


f is XOR $\Rightarrow$ K $\rightarrow$ [f] $\Rightarrow$ $1111 \oplus 1111 = 0000$



2020_09_22

- Consider the following feistel scheme

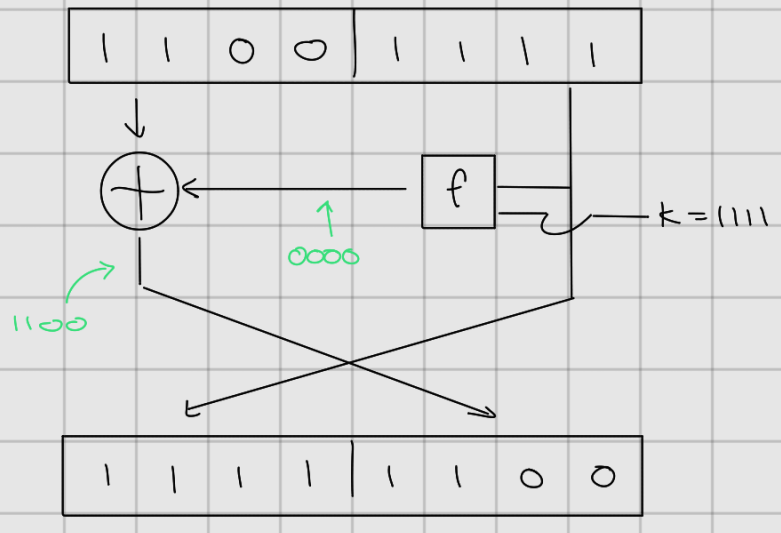


$B = 11001111$

$k = 1111$

$Y = ?$

A simple feistel network has the following schema:



the f is a XOR operator

- The same exercise with: $B = 01001111$

$k = 1111$

Solution: 11110100

SBOX WITH DES

2021_09_14

- Compute the value of $S_1(55)$ 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

INNER BIT → COLUMNS

55 → 1 1 0 1 1 1

OUTER BIT → ROWS

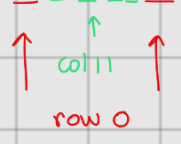
14

2020_09_22

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

$22 \rightarrow 16 + 4 + 2$

$\rightarrow 010110$ (we have 6 bits)



$S_1(22) = 12$

IP PERMUTATIONS WITH DES

2020_09_22

- Here the table 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: $IP^2 = IP \circ IP$

RECAL FROM THEORY:

The IP and IP^{-1} are used to provide difusion in the input text, it means that they spread the inputs among different data blocks so that a small modification to a portion of the plaintext has visible effects on all the chipertext
They are used as transposition operators and each element is a map to another one that corresponds to its index.

PROCEDURE:

In this situation the IP matrix has to be applied to itself and not to a plaintext (since we have $IP \circ IP$)

First row $\left[IP[58], IP[50], IP[42], IP[34], IP[26], IP[18], IP[10], IP[2]\right]$

$= [55, 53, 51, 49, 56, 54, 52, 50]$

↑
Apply the first row to IP itself means finding the elements with the indexes of the first row

RSA COMPUTATION

2021_09_19

- RSA parameters $p = 5$ $q = 11$. What is a valid combination for RSA?

a. $e = 12$ $M = 6$
b. $e = 17$ $d = 33$ $M = 6$ $C = 41$
c. $e = 11$ $d = 11$ $M = 6$ $C = 16$

PROCEDURE:

Recall that: RSA is composed of 3 things

- $Gen(\lambda)$
- $Enc_{pk}(m)$
- $Dec_{sk}(c)$

So we need 3 elements and we have to specify details:

$Gen(\lambda) \rightarrow$ chose p, q (prime numbers of λ bits),

compute $N = p \cdot q$ and $\phi(N) = (p-1)(q-1)$. Pick $e \in \mathbb{Z}^*_{\phi(N)}$

and compute $d = e^{-1} \bmod \phi(N)$ set $pk = (N, e)$

and $sk = (\phi(N), d)$

$Enc \rightarrow m \in \mathbb{Z}_N \Rightarrow c = m^e \bmod N$

$Dec \rightarrow m = c^d \bmod N$

Back to the exercise:

Analyze $e = \{12, 17, 11\}$

OPTION 1 $\Rightarrow$ $e = 12$

$d = e^{-1} \bmod \phi(N)$ the inverse exists only if

$\gcd(e, \phi(N)) = 1 \rightarrow \gcd(12, 40) = 4$ ✗✗✗

OPTION 2 $\Rightarrow$ $e = 17$

$d = e^{-1} \bmod \phi(N) \rightarrow \gcd(e, \phi(N)) = 1$ ✓ NICE

Now we have to find d and we need EEA

$40 = 2 \cdot 17 + 6$

$17 = 2 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1$

$5 = 5 \cdot 1 + 0$

START FROM HERE

$1 = 6 - 1 \cdot 5$

$1 = 6 - 1 \cdot (17 - 2 \cdot 6)$

$= -1 \cdot 17 + 3 \cdot 6$

$1 = -1 \cdot 17 + 3(40 - 2 \cdot 17)$

$= -7 \cdot 17 + 3 \cdot 40$

THIS IS THE INVERSE $\Rightarrow$ $-7 + 40 = 33$

So 33 is a match and we have to check the other parameters

Check M and C , M is the message itself that in option 2 is m=6

$$C = m^e \bmod N = 6^{17} \bmod 55 \qquad N = qp = 55$$

$17 \rightarrow 10001$

from LSB to MSB , base is 6 , and res = 1

1. $1 \rightarrow 1 \cdot 1 \bmod 55 = 1$

   $1 \cdot 6 \bmod 55 = 6$

2. $0 \rightarrow 6 \cdot 6 \bmod 55 = 36$

3. $0 \rightarrow 36 \cdot 36 \bmod 55 = 31$

4. $0 \rightarrow 31 \cdot 31 \bmod 55 = 26$

5. $1 \rightarrow 26 \cdot 26 \bmod 55 = 16$

   $16 \cdot 6 \bmod 55 = 41$ ✓

Note

Here every time you find a one you square and then multiply by base result

OPTION 2 IS RIGHT AND OPTION 3 IS NOT

ELLIPTIC CURVE DIFFIE HELLMAN

2020_07_21

- 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 ECDH to obtain the key session k. Alice secret key is $sk_A = 5$, Bob's secret key is $B = 12$. What is the session key?

PROCEDURE

From theory:

ALICE	BOB
pick A	pick B
$pA = A \cdot G = (x_A, y_A)$	$pB = B \cdot G = (x_B, y_B)$
	$\xrightarrow{pA}$
	$\xleftarrow{pB}$
$k_A = A \cdot pB$	$k_B = B \cdot pA$

$$k = k_A = k_B$$

What we know from the text is $A=5$ $B=12$ and $G(2,7)$

Take into account that:

- The curve is $y^2 = x^3 + 7$ $\mathbb{Z}_{17}$ → So it will have integer coordinates mod 17
- G is a generator so if we keep adding itself it will generate the entire curve.

We start from calculating Alice' pub key

$pk_A = A \cdot G = 5 \cdot G$ THIS IS THE SCALAR MULTIPICATION OF THE GENERATOR G BY A

we can decompose it into: $2G + 2G + G$

note that $2G$ is $G+G$ and so we can perform standard

EC addition of points

NOTE: THE EXERCISE PROVIDES US WITH THE ADDITION TABLE OF THE ELLIPTIC CURVE

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

$K = 12pB = \ldots = (5,8)$
$= 12pA = \ldots = (5,8)$

BABY CIPHER EXERCISE

2022_06_27

- Let $Enc^1_k(P) = k \oplus P$ be the Vernam or XOR cipher of 3bit blocks. Let $Enc^2_k(P) = k \boxplus P$ be the multiplication cipher modulo $8 = 2^3$ where k, P are binary elements of $\mathbb{Z}_8$ (ex: [011] is 3).

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

knowing that $Enc_k(3) = 4$ $Enc_k(1) = 7$ find k_2 and k_1

RECALL FROM THEORY:

Vernam cipher $\rightarrow$ $P \oplus k = C \Leftrightarrow P = C \oplus k$

Mutiplication cipher $\rightarrow$ $P \boxtimes k = C \rightarrow$