



INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO



Cryptography

Guía de ejercicios

January, 2026

1. Unit I

Please solve the following exercises using only a pocket calculator. Solve them and if you have questions please ask for help. You DON'T NEED to upload your answers in Teams.

- For each of the following exercises, give the result as an integer greater or equal than 0 and less than the module. For example $-3501 \bmod 7 = 6$.
 - $-81 \bmod 11$
 - $-162 \bmod 13$
 - $-10002 \bmod 17$
 - $-5303 \bmod 12$
 - $-3111123 \bmod 6$
- For each set, list those elements that have a multiplicative inverse. For example in \mathbb{Z}_9 , 5 has multiplicative inverse: 2, since $5 * 2 \bmod 9 = 1$.
 - \mathbb{Z}_7 ,
 - \mathbb{Z}_7^*
 - \mathbb{Z}_8
 - \mathbb{Z}_{17}
 - \mathbb{Z}_{14}
 - \mathbb{Z}_{40}^*
 - \mathbb{Z}_{36}
 - \mathbb{Z}_{30}^*
- Using the extended Euclidean algorithm,
 - find $2^{-1} \bmod 27$, $25^{-1} \bmod 27$.
 - find $7^{-1} \bmod 30$, $11^{-1} \bmod 30$, $4^{-1} \bmod 30$.
- Assume that each of the following values of n is a size alphabet. Find 5 different valid keys $K = (a, b)$ for the affine cipher, for each n and use the extended Euclidean algorithm to find $a^{-1} \bmod n$

a) $n = 21$

b) $n = 19$

c) $n = 30$

5. For each of the following pair of values run Algorithm 2 and list the content of variables in each iteration $u, v, x_1, x_2, q, r, x, y$. What is the output for each pair (a, p) ?

a) $a = 5, p = 13$

b) $a = 7, p = 26$

c) $a = 11, p = 30$

d) $a = 8, p = 15$

e) $a = 9, p = 14$

Algorithm2(a, p)

```

1.   $u \leftarrow a; v \leftarrow p$ 
2.   $x_1 \leftarrow 1, x_2 \leftarrow 0;$ 
3.  while  $u \neq 1$  do
3.1.   $q \leftarrow \lfloor v/u \rfloor, r \leftarrow v - qu, x \leftarrow x_2 - qx_1;$ 
3.2.   $v \leftarrow u, u \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x,;$ 
4.  return  $(x_1 \bmod p)$ 
```

6. Do the following operations only with a pocket calculator. Consider that sometimes it is not possible to do the operation.

a) $(3 * 2/5) \bmod 7$

b) $((19 + 1/5) * 3 - 4/3) \bmod 11$

c) $(5/6 + (-5 - 8)/4) \bmod 8$

d) $(11/4 * 5/2) \bmod 5$

e) $(-8 + 13 * (-2)/11) \bmod 22$

7. The function $\phi(n)$ is called the Euler phi function and denotes the number of integers between 1 and n for $n \geq 1$ which are relatively prime to n . We can calculate $\phi(n)$ using the following properties:

- If p is a prime number, then $\phi(p) = p - 1$
- If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m) \cdot \phi(n)$
- If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization of n , then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$$

Using the previous definition calculate :

a) $\phi(11)$

b) $\phi(101)$

c) $\phi(22)$

d) $\phi(21)$

e) $\phi(30)$

f) $\phi(42)$

8. If the size of the alphabet is 30, how many different keys are available for affine cipher. Tip: the Euler's function can help you to find this number.
9. If the size of the alphabet is 19, how many different keys are available for affine cipher. Tip: the Euler's function can help you to find this number.
10. If the size of the alphabet is 21, how many different keys are available for affine cipher. Tip: the Euler's function can help you to find this number.
11. For each of the following permutations, compute the inverse permutation.

a) $\pi(x)$

5	3	1	2	4	6
---	---	---	---	---	---

b) $\pi(x)$

7	1	6	2	5	3	4
---	---	---	---	---	---	---

c) $\pi(x)$

10	2	4	9	1	6	8	7	3	5
----	---	---	---	---	---	---	---	---	---

12. Given the irreducible polynomial $1 + x + x^7$, which finite field can we construct with it? How many elements does it have?
13. List the elements in $\text{GF}(2^5)$ using the irreducible polynomial $1 + x^2 + x^5$. Represent each element, as a polynomial, as a binary and in hexadecimal. Write the multiplication table and find the multiplicative inverse for each element.
14. Compute the following multiplications, write the result as a polynomial, as a binary string and in hexadecimal.
 - $(x^2 + 1) * (x^3 + x^2 + 1) \text{ mód } x^4 + x^3 + 1$
 - $(x^2 + 1) * (x + 1) \text{ mód } x^4 + x^3 + 1$
15. To do arithmetic over a binary finite field $\text{GF}(2^5)$, we need an irreducible polynomial.
 - a) Which of the following irreducible polynomials we must use:
 - $x^4 + x^3 + 1$,
 - $x^5 + x^3 + 1$
 - $x^6 + x^5 + x^2 + x + 1$?
 - b) How many elements are in this field?
 - c) Use the irreducible polynomial you chose in a) to write down the mathematical expresion (as we explained in class) to do the operation $x * f(x)$ if $f(x) \in \text{GF}(2^5)$. Use only the binary representation of $f(x)$ and bitwise operations.
 - d) Use the mathematical expression you gave in c) and bitwise operations to multiply $f(x) * g(x)$, where $f(x) = x^4 + x^2 + 1$ and $g(x) = x^2 + 1$. Give the result in binary, in hexadecimal and as a polynomial.

2. Unit II

1. We know that the constants used in the *key expansion* of AES are obtained as follows:

$$\begin{aligned}
 RC[1] &= x^0 \text{ mód } x^8 + x^4 + x^3 + x + 1 \\
 RC[2] &= x^1 \text{ mód } x^8 + x^4 + x^3 + x + 1 \\
 RC[3] &= x^2 \text{ mód } x^8 + x^4 + x^3 + x + 1 \\
 &\vdots \\
 RC[8] &= x^7 \text{ mód } x^8 + x^4 + x^3 + x + 1 \\
 RC[9] &= x^8 \text{ mód } x^8 + x^4 + x^3 + x + 1 = x^4 + x^3 + x + 1
 \end{aligned}$$

Compute the constants for rounds 11, 12, 13 y 14, i.e. $RC[11]$, $RC[12]$, $RC[13]$, $RC[14]$, write the result in binary and in hexadecimal.

2. Use the multiplicative inverse table for $GF(2^8)$ in Figure 1. Use the multiplication with bitwise operations to show that $02 * 8D = 01$ and that $B0 * C0 = 01$. Include the detail of your calculations.

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

Figura 1: Multiplicative inverse table for $GF(2^8)$

3. See Figure 2
 - a) Describe the content of each of the following variables: L^{i-1} , R^{i-1} , f , K^i , L^i , R^i
 - b) What is the mathematical expression for L^i and R^i .
 - c) List three block ciphers that use this structure.
4. List five differences between AES and 3DES. (**Value: 2.0 points**)
5. We know that a block cipher E_k can only encipher a block of fixed size b . To encipher a plaintext M such that $|M| > b$ we need a mode of operation. Analyze the mode of operation shown in Figure 3 and answer the following questions:
 - a) Do the diagram to decipher a ciphertext C

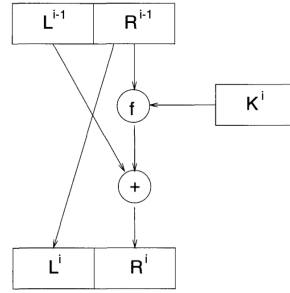


Figura 2: Feistel Network

- b) Write down the pseudocode to encipher a plaintext M . Please use the mathematical notation we explained in class.
- c) Write down the pseudocode to decipher a ciphertext C . Please use the mathematical notation we explained in class.

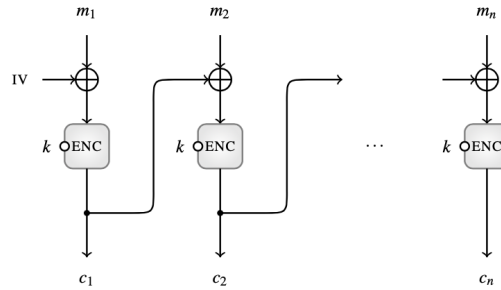


Figura 3: A mode of operation

6. Do the following matrix multiplication, Consider that the values are in hexadecimal and are elements of $GF(2^4)$ Use the irreducible polynomial $x^4 + x + 1$.

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix}$$

7. The following algorithm computes the round keys for AES, with a key of 128 bits. This algorithm do the following operations. ROTWORD(B_0, B_1, B_2, B_3) it makes a cyclic shift of 4 bytes to B_0, B_1, B_2, B_3 , i.e.

$$\text{ROTWORD}(B_0, B_1, B_2, B_3) = B_1, B_2, B_3, B_0,$$

SUBWORD(B_0, B_1, B_2, B_3) use the AES sbx to each byte B_0, B_1, B_2, B_3 , i.e.

$$\text{SUBWORD}(B_0, B_1, B_2, B_3) = B'_0, B'_1, B'_2, B'_3$$

$Rcon$ is an array of 10 words. These constants are in hexadecimal

Algorithm 3.6: KEYEXPANSION(*key*)**external** ROTWORD, SUBWORD $RCon[1] \leftarrow 01000000$ $RCon[2] \leftarrow 02000000$ $RCon[3] \leftarrow 04000000$ $RCon[4] \leftarrow 08000000$ $RCon[5] \leftarrow 10000000$ $RCon[6] \leftarrow 20000000$ $RCon[7] \leftarrow 40000000$ $RCon[8] \leftarrow 80000000$ $RCon[9] \leftarrow 1B000000$ $RCon[10] \leftarrow 36000000$ **for** $i \leftarrow 0$ **to** 3 **do** $w[i] \leftarrow (key[4i], key[4i + 1], key[4i + 2], key[4i + 3])$ **for** $i \leftarrow 4$ **to** 43 $\left\{ \begin{array}{l} temp \leftarrow w[i - 1] \\ \text{if } i \equiv 0 \pmod{4} \end{array} \right.$ **then** $temp \leftarrow \text{SUBWORD}(\text{ROTWORD}(temp)) \oplus RCon[i/4]$ $w[i] \leftarrow w[i - 4] \oplus temp$ **return** $(w[0], \dots, w[43])$

Given the AES key $K = 01000202 \ F0F0F0F0 \ 1B1B1B1B \ 52475252$. Which is the content of $w[0], w[1], w[2], w[3], w[4]$?

3. Unit IV

- Encipher and decipher using RSA for each of the following set of values. Use the extended euclidean algorithm to find the private key in each case
 - $p = 3; q = 11, e = 7; M = 5$
 - $p = 5; q = 11, e = 3; M = 9$
 - $p = 7; q = 11, e = 17; M = 8$
 - $p = 11; q = 13, e = 11; M = 7$
 - $p = 17; q = 31, e = 7; M = 2$
- Suppose you are attacking RSA, you have obtained the ciphertext $C = 10$ which was sent by a user with public key $(e, n) = (5, 35)$. Find the the corresponding plaintext M .
- A user has the RSA public key $(e, n) = (31, 3599)$ Find the corresponding private key d .
- Alicia y Bob are using the protocol Diffie-Hellman with a prime number $p = 71$ and a generator $g = 7$
 - a) If Alice uses the secret value $a = 5$, compute the value that Alice must sent to Bob, using the given a, g, p

- b) If Bob uses the secret value $b = 12$, compute the value that Bob must send to Alice, using the given b, g, p
 - c) Compute the secret that will obtain Alice and Bob at the end of the protocol
- 5. Consider the protocol Diffie-Hellman with a prime number $q = 17$ and a primitive element $\alpha = 3$
 - a) Do the calculations to show that 3 is a primitive element or generator of \mathbb{Z}_{17}
 - b) If Alice sends to Bob $y_A = 8$ find the secret value a such that $3^a \bmod 17 = 8$
 - c) If Bob sends to Alice $y_B = 7$ find the secret value b such that $3^b \bmod 17 = 7$
- 6. For each of the following pair of values, compute the secret that will obtain Alice and Bob if they use the Diffie-Hellman with a prime number $p = 467$ and $g = 2$. Do the calculations for both Alice and Bob to verify that your result is correct.
 - a) $a = 3; b = 5$
 - b) $a = 400; b = 134$
 - c) $a = 228; b = 57$
- 7. What cryptographic services provide RSA?
- 8. Why is not a good idea to use RSA to encipher a file with Mb, Gb or TB of information?
- 9. Show that every time we encipher a plaintext using RSA, we will be able to decipher the corresponding ciphertext.
- 10. If we are trying to solve the discrete logarithm problem, what is the input data? What is the output data?
- 11. How can we argue about the security of the Diffie-Hellman protocol?
- 12. How can we argue about the security of RSA?
- 13. Why do we say that RSA is a deterministic algorithm?