Cryptography

GROUP ACTIVITY

THEORETICAL CONTENTS **3**
1. Cryptography **3**
2. Private key cryptography **4**
a. Monoalphabetic cyphers 4
i. Caesar's algorithm 4
ii. Affine cipher 5
iii. General monoalphabetic cipher 6
b. Polyalphabetic ciphers 7
i. Vigénere's cipher 7
3. Public key cryptography **9**
a. The RSA algorithm 11
EXERCISES **16**

THEORETICAL CONTENTS

1. Cryptography

Cryptography (from Ancient Greek κρυπτός, kryptós, "hidden, secret"; and γράφειν, graphein, "to write"; literally "secret writing") is the art or science of ciphering or deciphering information using techniques that enable an exchange of messages in such a way that they can only be read by the people to whom they are directed.

The end goal of cryptography is, in the first place, to guarantee the secret communication between two entities (people, organizations, etc.) and, secondly, to ensure that the information that is sent is authentic in two ways: that the identity of the sender is true, and that the content of the message (usually called cryptogram) has not been modified in transit.

The focus of this unit is set on the first goal of cryptography, that is, to analyze the different cryptographic mechanisms and ways of ciphering and deciphering information. We will study algorithms that, given a message $M = a_1 a_2 \dots a_k$ composed by different symbols (a_i), transform it into another ciphered message $C = c_1 c_2 \dots c_r$ in a reversible manner, that is, algorithms that are also capable of translating the ciphered message back into the original message.

There are two historical eras in the field of cryptographic mechanisms. In the first one, we consider systems prior to WWII, prior to the first computers. The mechanisms belonging to this first era were implemented and used through pen and paper. The inception of computers made the messages that employed these codes trivial to decipher, and hence no longer useful to guarantee the secret of communications, causing these methods to rapidly fall into disuse. This first era is called classic cryptography, or private key cryptography.

The transition towards modern cryptography or public key cryptography started during WWII, when the allied intelligence services were able to decipher the mechanisms of the machine used by Nazi Germany, ENIGMA.

2. Private key cryptography

Private key algorithms, also called symmetrical algorithms, are characterized by the usage of the same key for the ciphering and deciphering of messages.

a. Monoalphabetic cyphers

Monoalphabetic cyphers are cryptographic algorithms that establish a correspondence between the symbols of the original message and the ciphered message in a unique way (that is, two symbols that are equal between them are translated into other symbols that are equal between them). These algorithms do not rearrange the symbols that compose the message when it is ciphered.

$$\begin{aligned} & M \leftrightarrow C \\ & a_1 \leftrightarrow c_1 \\ & a_2 \leftrightarrow c_2 \quad \text{and if } a_i = a_j \rightarrow c_i = c_j \\ & \quad \vdots \\ & a_k \leftrightarrow c_k \end{aligned}$$

i. Caesar's algorithm

It is one the simplest cryptographic algorithms. It takes its name from Julius Caesar, who used the algorithm to cipher his messages. The algorithm consists in swapping a letter for a letter 3 spaces above it in the alphabet. If we consider an alphabet of m letters and assign non-negative integer numbers to the letters by their order:

A	*B*	*C*	*D*	…
0	1	2	3	…

The cryptographic transformation would be:

$$C = M + 3 \, mod \, m$$

Where C represents the ciphered version of M, M is the number that corresponds to the letter in the original message by the defined table, and m is the number of letters in the alphabet that we consider in order to build our messages. To decipher the message, it is enough to subtract 3 module m:

$$M = C - 3 \, mod \, m$$

Example

Cipher through Caesar's algorithm the message 'VINI VIDI VINCI' considering the standard 26-letter English alphabet. First, we take the table that assigns numbers to each letter in the alphabet:

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
0	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

MESSAGE		$C = M + 3 \, mod \, m$		*CIPHERED MESSAGE*
V	21	$24 = 21 + 3 \, mod \, 26$	24	Y
I	8	$11 = 8 + 3 \, mod \, 26$	11	L
N	13	$16 = 13 + 3 \, mod \, 26$	16	Q
I	8	$11 = 8 + 3 \, mod \, 26$	11	L
V	21	$24 = 21 + 3 \, mod \, 26$	24	Y
I	8	$11 = 8 + 3 \, mod \, 26$	11	L
D	3	$6 = 3 + 3 \, mod \, 26$	6	G
I	8	$11 = 8 + 3 \, mod \, 26$	11	L
V	21	$24 = 21 + 3 \, mod \, 26$	24	Y
I	8	$11 = 8 + 3 \, mod \, 26$	11	L
N	13	$16 = 13 + 3 \, mod \, 26$	16	Q
C	2	$5 = 2 + 3 \, mod \, 26$	5	F
I	8	$11 = 8 + 3 \, mod \, 26$	11	L

The ciphered message takes the form: 'YLQL YLGL YLQFL'

ii. Affine cipher

The affine cipher is a generalization of Caesar's algorithm. Equally to Caesar's algorithm, the affine cipher considers an alphabet of m letters, and assigns non-negative integer numbers to the letters by order of appearance:

A	*B*	*C*	*D*	…
0	1	2	3	…

The key k for the cipher is given by the pair $k = (a, b)$, where $a, b \in \mathbb{Z}_m$.

In this case, the cryptographic transformation takes the form $C = aM + b \, mod \, m$, where M is the number that corresponds to the letter of the original message according to the prior table and C represents the cryptographic transformation of M. To decipher the message, we use $M = a^{-1} \cdot C - a^{-1} \cdot b \, mod \, m$

Note

In order to be able to decipher messages ciphered by the affine cipher, it is necessary for a to be invertible module m.

Example

Decipher the message 'KAM MA', ciphered through the affine cipher with key $(9,4)$ and the standard 26-letter English alphabet.

In this case, $a = 9$ and $b = 4$. In order to be able to decipher the message, we must find the inverse of $a = 9\,mod\,26$. We develop the Euclidean algorithm to invert the process and reach Bézout's identity, from which we can find the inverse that we are looking for.

$$26 = 9 \cdot 2 + 8$$

$$9 = 8 + \boxed{1}$$

Observe that $gcd(26,9) = 1$ and then we can affirm that 9 has an inverse module 26.

$$1 = 9 - 8 = 9 - (26 - 9 \cdot 2) = 9 \cdot 3 - 26 = 9 \cdot 3\,mod\,26$$

Hence $a^{-1} = 3\,mod\,26$

In order to decipher the message, we must use the expression $M = a^{-1} \cdot C - a^{-1} \cdot b\,mod\,m$, tailored for the values of the problem: $M = 3 \cdot C - 3 \cdot 4\,mod\,26$

We take the table that assigns numbers to each letter of the alphabet in order to interpret letters as numbers, thus becoming able to apply congruencies.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
0	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

CIPHERED MESSAGE	*C*	$M = 3 \cdot C - 3 \cdot 4\,mod\,26$	*M*	*pESSAGE*
K	10	$18 = 3 \cdot 10 - 3 \cdot 4\,mod\,26$	18	S
A	0	$14 = -3 \cdot 4\,mod\,26$	14	O
M	12	$24 = 3 \cdot 12 - 3 \cdot 4\,mod\,26$	24	Y
M	12	$24 = 3 \cdot 12 - 3 \cdot 4\,mod\,26$	24	Y
A	0	$14 = -3 \cdot 4\,mod\,26$	14	O

The original message was: 'SOY YO' *(Spanish for IT'S ME)*

iii. General monoalphabetic cipher

For each letter of the alphabet, another symbol or letter is chosen, such that the selection of the cipher is never repeated. In this case, the key is formed by the table where the substitutions are specified. For instance:

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Using the standard 26-letter English alphabet, we have $26!$ different keys.

b. Polyalphabetic ciphers

In polyalphabetic ciphers, the substitution applied to each character varies depending on the position that the character occupies within the non-ciphered text. The most typical example of polyalphabetic cipher, which owes its name to Blaise Vigénere, dates from the 16th century.

i. Vigénere's cipher

Considering again an alphabet with m symbols, the key is built through a sequence of symbols that belong to the given alphabet:

$$k = (k_0, k_1, k_2, \dots, k_{d-1})$$

The cipher function is then as follows:

$$c_i = m_i + k_{i \bmod d} \bmod m$$

Being m_i the number assigned to the i-th symbol of the text that must be ciphered and c_i the i-th symbol of the ciphered text.

To decipher a message ciphered through Vigénere, function $m_i = c_i - k_{i \bmod d} \bmod m$ is used.

Example

Cipher message 'SOY YO' *(Spanish for IT'S ME)* through Vigénere's cipher with the standard 26-letter English alphabet and key $k = \{2,10,12\}$

In this case $k_0 = 2, k_1 = 10, k_2 = 12$ and $d = 3$.

We take the table that assigns numbers to each letter of the alphabet in order to interpret letters as numbers and thus be able to apply congruencies.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
0	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

MESSAGE	m_i	$i \bmod d$	$k_{i \bmod d}$	$c_i = m_i + k_{i \bmod 3} \bmod m$	c_i	*CIPHERED MESSAGE*
S	18	$0 = 0 \bmod 3$	*2*	$20 = 18 + 2 \bmod 26$	20	U
O	14	$1 = 1 \bmod 3$	*10*	$24 = 14 + 10 \bmod 26$	24	Y
Y	24	$2 = 2 \bmod 3$	*12*	$10 = 24 + 12 \bmod 26$	10	K
Y	24	$0 = 3 \bmod 3$	*2*	$0 = 24 + 2 \bmod 26$	0	A
O	14	$1 = 4 \bmod 3$	*10*	$24 = 14 + 10 \bmod 26$	24	Y

The ciphered message takes the form: 'UYKAY'

To decipher the message, it is enough to use the appropriate decipher function particularized to the values of the example: $m_i = c_i - k_{i\,mod\,3}\ mod\ m$

CIPHERED MESSAGE	c_i	$i\ mod\ d$	$k_{i\,mod\,d}$	$m_i = c_i - k_{i\,mod\,3}\ mod\ m$	m_i	*MESSAGE*
U	20	$0 = 0\ mod\ 3$	*2*	$18 = 20 - 2\ mod\ 26$	18	S
Y	24	$1 = 1\ mod\ 3$	*10*	$14 = 24 - 10\ mod\ 26$	14	O
K	10	$2 = 2\ mod\ 3$	*12*	$24 = -2 = 10 - 12\ mod\ 26$	24	Y
A	0	$0 = 3\ mod\ 3$	*2*	$24 = 0 - 2\ mod\ 26$	24	Y
Y	24	$1 = 4\ mod\ 3$	*10*	$14 = 24 - 10\ mod\ 26$	14	O

3. Public key cryptography

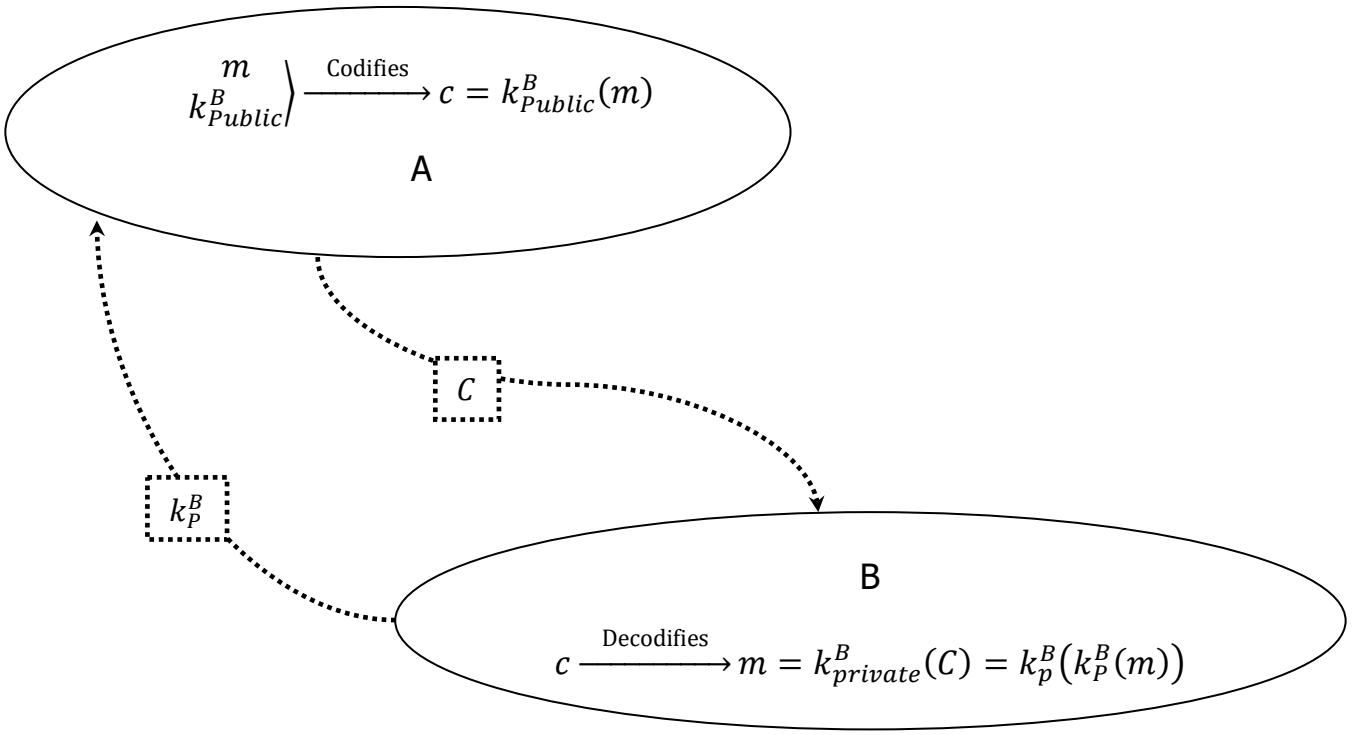
Public key algorithms, also called asymmetric algorithms, were introduced by W. Diffie y M. Hellman in the 70s decade. They have proven their usefulness to be leveraged in insecure communications networks such as the Internet. The main difference between these cryptographic algorithms and symmetric algorithms is that there is not a single key to cipher and decipher messages. Rather, the cryptographic key is formed by a pair of keys, $k = (k_p, k_P)$, respectively called private key and public key.

Public key K_P, is the one that is made known and is used to cipher messages. Private key K_p is used to decipher the messages and must only be known by the owner of the keys. In order for a user to be able to send ciphered information to another user, the sender must know the public key of the receiver.

Suppose that user A wants to send a message m to user B through an asymmetric algorithm. To use an asymmetric algorithm, user B must have a pair of private and public keys (k_p^b, k_P^B). A asks B for the public key, and codifies the message using that key and the appropriate algorithm.

Be it $c = k_P^B(m)$ the obtained cryptogram and consider that A sends the cryptogram to B, who can decipher the message through the private key:

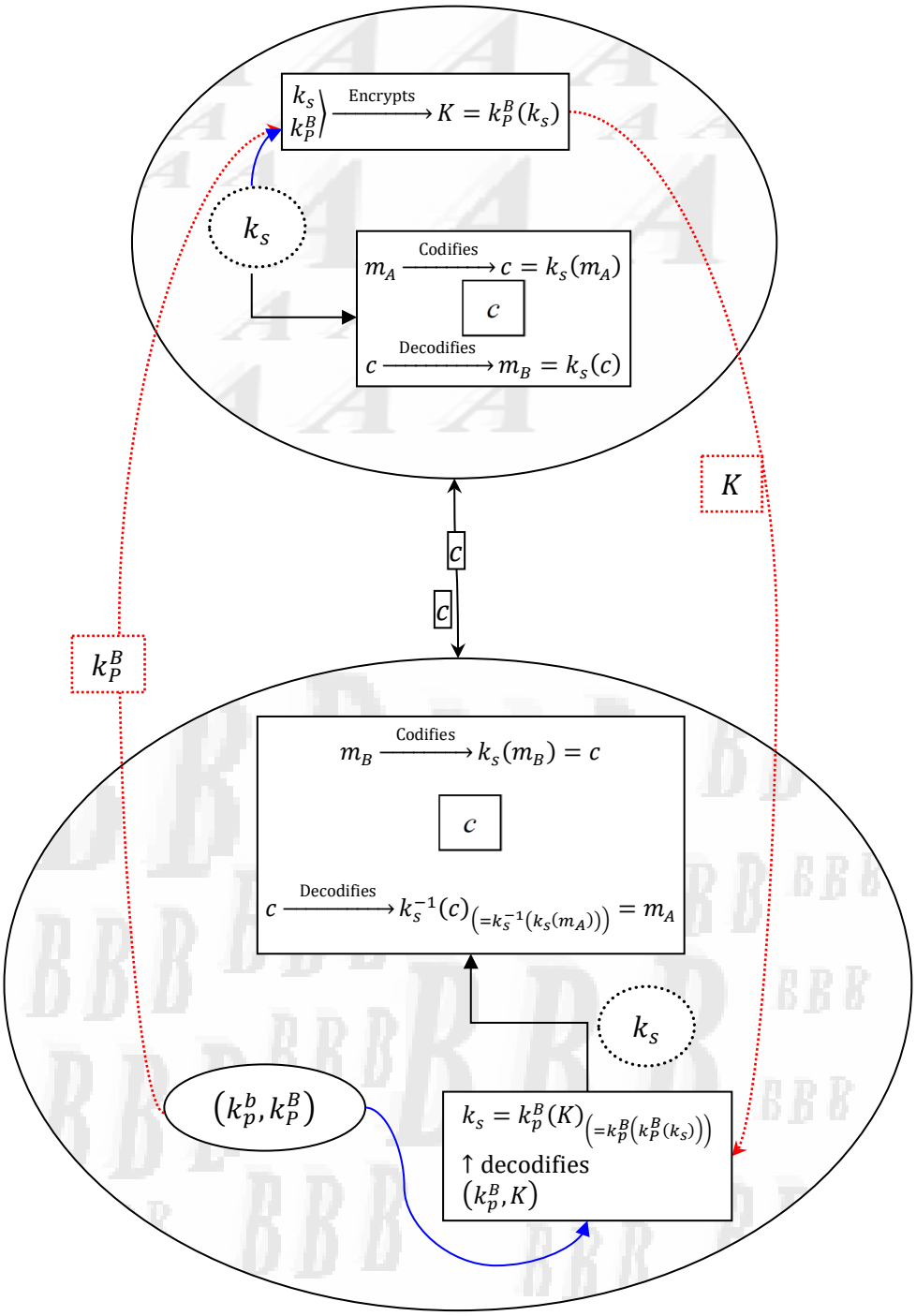
$m = k_P^B(C) = k_P^B\left(k_p^B(m)\right)$.



Observe that through these methods, only a user that has a pair of keys can receive ciphered messages. In other words, in order to use asymmetric algorithms, each user must have a pair of keys to be able to establish secure communications. Additionally, through these methods, users do not have to agree on a common key.

A potential attacker who wants to decipher a cryptogram (ciphered message) must deal with the resolution of complex mathematical problems, on which the security of the methods is based. The main

issue with asymmetrical algorithms is that they need a considerable key length in order to result safe. For instance, symmetrical algorithms consider a 128-bit key as secure, while asymmetrical algorithms recommend using 1024-bit keys at least (except for a special kind of algorithm based on elliptic curves).



In addition, the calculus complexity carried by asymmetric algorithms makes them considerably slower than symmetrical cipher algorithms. In practice, public key algorithms are used together with private key algorithms. Messages are codified through a symmetric algorithm that uses a key called **session key** that

must be different each time a communication between two users is established. The session key is then codified through asymmetric cryptography.

Suppose user A wants to establish secure communications with user B. A randomly creates a session key k_s for a particular symmetric algorithm. A send B the session key, encrypting it through the public key provided by B, k_P^B, and an asymmetric algorithm. B receives the encrypted session key, $K = k_P^B(k_s)$, and deciphers it through the use of the private key: $k_s = k_p^B(K) = k_p^B\left(k_P^B(k_s)\right)$. This way, the two users have now established a common session key and can send messages ciphered through a symmetric algorithm. Going forwards, if A wants to send message m_A to B, a cryptogram $k_s(m_A)$ will be sent. Analogously, messages sent by B to A will be cryptograms $k_s(m_B)$, and in order to read them, A will have to decipher them using the session key: $m_B = k_s^{-1}\left(k_s(m_B)\right)$.

Among all the public key algorithms, the most widespread is the RSA algorithm, for it is one of the easiest to understand and implement. The algorithm is based on the difficulty of factorizing big numbers.

a. The RSA algorithm

The algorithm owes its name to its inventors: R. Rivest, A. Shamir, and L. Adleman. It was under a patent license until September of 2000, and thus its commercial usage was restricted until that date. It is considered to be one of the most secure asymmetric algorithms, even when its alleged security has yet to be proven or refuted. It has been able to overcome numerous kinds of attacks.

The RSA key, formed by a pair of keys consisting of a public and a private key, is calculated from a number that is obtained as a product of two large prime numbers. Its secureness resides in the difficulty to factorize large numbers.

The public and private keys of RSA are created as follows:

1. Two large prime numbers, p and q, are chosen.
2. Number $n = p \cdot q$ is obtained.
3. $\Phi(n) = (p-1)(q-1)$ is calculated.
4. A number e is chosen, such that $gcd\left(e, \Phi(n)\right) = 1$.
5. The inverse of e module $\Phi(n)$ is calculated: $d = e^{-1}\ mod\ \Phi(n)$
6. The public key will be $K_{Public} = (e, n)$, and the private key will be $k_{private} = (d, n)$

To encode or cipher a message m from the public key $K_P = (e, n)$, we use cipher function $c = m^e\ mod\ n$

To decipher a cryptogram c we use the private key $K_p = (d, n)$ in the decipher function $m = c^d\ mod\ n$

Notes

✓ Observe that the latter equality is verified if the following chain of equalities can be verified:

$$c^d = (m^e)^d = m^{e\cdot d} =_{d=e^{-1} mod\ \Phi(n)} m^{e\cdot e^{-1} mod\ \Phi(n)} = m^{1+k\cdot\Phi(n)} = m\cdot\left(m^{\Phi(n)}\right)^k =_{\substack{m^{\Phi(n)}=1\ mod\ n \\ (Euler's\ theorem)}} m\ mod\ n$$

To that extent, the following equalities must be verified:

1. $e \cdot d = 1\, mod\, \Phi\,(n)$
2. $m^{e\cdot d} = \left(m^{\Phi(n)}\right)^k \cdot m\, mod\, n$
3. $m^{\Phi(n)} = 1\, mod\, n$

This is where our election of e and d and Euler's theorem come into play:

1. Taking e with $gcd\left(e, \Phi(n)\right) = 1$ we can ensure that it is inversible, and then we can take its inverse $d = e^{-1}\, mod\, \Phi\,(n)$. Then, it is immediate that $e \cdot d = e \cdot e^{-1} = 1\, mod\, \Phi\,(n)$.
2. By the definition of congruence, this means that $\Phi(n)|_{e\cdot d-1}$, and that $\Phi(n)$ divides $e \cdot d - 1$, ensuring that $\exists k \in \mathbb{Z}$ such that $d \cdot e - 1 = k \cdot \Phi(n) \Rightarrow d \cdot e = 1 + k \cdot \Phi(n)$. Hence, we have that $m^{e\cdot d} = m^{1+k\cdot\varphi(n)} = m^{k\cdot\varphi(n)} m^1 = \left(m^{\varphi(n)}\right)^k m\, mod\, n$
3. Euler's theorem states that $mcd(m,n) = 1 \Rightarrow m^{\varphi(n)} = 1\, mod\, n$. Substituting this equality in the prior point we have that $m^{e\cdot d} = \left(m^{\varphi(n)}\right)^k m = 1^k m = m\, mod\, n$.

Notes

✓ Through the last equality we can affirm that the RSA algorithm works as long as we codify messages m such that $gcd(m,n) = 1$, that is, coprime with n. In any other case, we could not ensure the correctness of the deciphered message.

✓ This is not problematic. Usually, we want to codify the session key of a symmetric algorithm, which is then leveraged to codify the message. These keys are normally 128 bits long, making them numbers of the order of 1040, while p and q are numbers longer than 1024 bits, making them of the order of 10300, making m smaller than p and q and causing m and n to be coprime numbers $(m \ll p, q < n)$.

✓ In order to be able to decipher a cryptogram, an attacker must know the private key $k_p = (d,n)$. To that extent, the attacker must know the public key $k_P = (e,n)$ and the value of $\Phi(n)$.

✓ The secureness of the algorithm is based upon the difficulty to calculate $\Phi(n)$ without knowing the factorization of n, and thus, in the difficulty of factorizing n when it is a large number.

✓ This is the reason why p and q must be sufficiently large and unknown, and why $\Phi(n)$ must never be made known. In any of those scenarios, the private key might be uncovered, and the messages would be deciphered.

✓ If we can factorize $n = p \cdot q$ and then calculate $\Phi(n) = (p-1)(q-1)$, calculating the private key would be as easy as calculating $d = e^{-1}\, mod\, \Phi\,(n)$ through Bézout's identity.

Example 1

Two careless users take as public key $K_P = (37,221)$ and send each other cryptogram 159 ciphered through RSA. What is the message they sent each other?

In the example, the users have been careless, since they have used as key a number that can be easily factorized: $221 = 13 \cdot 17$. Observe that we do not need to use any factorization algorithm, since it is enough to try to divide the number with the prime numbers below its square root ($\sqrt{221} \simeq 14{,}86$). Now, it is easy to calculate $\Phi(221) = (13-1)(17-1) = 12 \cdot 16 = 192$ from the factorization in prime numbers. Observe that $mcd(e, \Phi(n)) = mcd(37,192) = 1$, to verify this it is enough to apply the Euclidean algorithm:

$$192 = 5 \cdot 37 + 7$$
$$37 = 5 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$

Using these equalities, we can calculate the following Bézout's identity (expressing $mcd(37,192) = 1$ as a linear combination of 37 and 192)

$$\left.\begin{array}{l} 192 = 5 \cdot 37 + 7 \\ 37 = 5 \cdot 7 + 2 \\ 7 = 3 \cdot 2 + 1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} 7 = 192 - 5 \cdot 37 \\ 2 = 37 - 5 \cdot 7 \\ 1 = 7 - 3 \cdot 2 \end{array}\right\} \Rightarrow$$

$$1 = 7 - 3 \cdot \mathbf{2} = 7 - 3 \cdot (\mathbf{37} - \mathbf{5} \cdot \mathbf{7})$$

$$= -3 \cdot 37 + 16 \cdot \mathbf{7} = -3 \cdot 37 + 16 \cdot (\mathbf{192} - \mathbf{5} \cdot \mathbf{37})$$

$$= 16 \cdot 192 - 83 \cdot 37 \Rightarrow \mathbf{1} = \mathbf{16} \cdot \mathbf{192} + (\mathbf{-83}) \cdot \mathbf{37}$$

Taking congruencies module 192 we have that $1 = (-83) \cdot 37 \, mod \, 192 \Rightarrow 37^{-1} = -83 = 109 \, mod \, 192$

Hence, we have the value of $d = 109 \, mod \, 192$, the part of the private key that we needed to decipher the message. Now, deciphering the message is reduced to calculating $159^{109} \, mod \, 221 = 146 \, mod \, 221$. Hence, the message that the users sent each other is 146.

Example 2

Users A and B want to start a secure session to share a huge amount of data. To that extent, they have designed the following hybrid cipher system: B will send A the session key (a, b) to cipher data through affine substitution with the 27-symbol Spanish alphabet (including the *ñ* character). To send the session key, they will use the RSA algorithm and a public key provided by A.

1. A is a careless user and has used public key $K_P = (19{,}161)$. Find his private key.
2. B has sent the session key to user A. As an attacker, you have intercepted the ciphered message, finding out that the first value is 23 and the second value is 48. Decipher the key.
3. Now that you know the session key, decipher the message that A sent B confirming the reception of the key: MXUMHWXÑRPH. Note: the second message that A sent B was RAMONES

Solution

1. Factorization of 81

--> fermat(7*23)

(n+1)/2 = 81.

!x e=x^*x-n z=2x+1 y=sqrt(e) !

13. 8. 27. 2.8284271

14. 35. 29. 5.9160798

15. 64. 31. 8.

The number is not a prime number, and there is a factorization through Fermat's method. The values of the two factors are a=7 and b=23

Calculation of the private key:

$$\left.\begin{array}{l} n = 161 = 7 \cdot 23 \\ \Phi(n) = 6 \cdot 22 = 132 \\ 19^{-1} = 7\, mod\, 132 \end{array}\right\} \rightarrow k_p = (7{,}161)$$

-->inversomod(19,132)

The mcd of 19 and 132 is 1

Bézout's identity takes the form (19)*(7)+(132) *(-1)=1

Then, the inverse of 19 mod 132 is 7

2. Calculation of the session key through RSA deciphering:

$$23^7 = 23\, mod\, 161$$

$$48^7 = 13\, mod\, 161$$

Then, the key is $(a, b) = (23{,}13)$

3. Deciphering the message through affine substitution

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

CIPHER $c_i = am_i + b \, mod \, 27$,$(a, b) = (23,13)$,

$$\left.\begin{matrix} 27 = 23 \cdot 1 + 4 \\ 23 = 4 \cdot 5 + 3 \\ 4 = 3 \cdot 1 + 1 \end{matrix}\right\} \begin{cases} 1 = 4 - 3 = 4 - (23 - 4 \cdot 5) = \\ = 6 \cdot 4 - 23 = 6(27 - 23) - 23 = \\ = 27 \cdot 6 + (-7) \cdot 23 = (-7) \cdot 23 \, mod \, 27 \rightarrow 23^{-1} = -7 = 20 \, mod \, 27 \end{cases}$$

DECIPHER $m_i = a^{-1}(c_i - b) = 20(c_i - 13) =_{-13 \cdot 20 = 10 \, mod \, 27} 20c_i + 10 \, mod \, 27$

CIPHER	c_i	$m_i = 20c_i + 10 \, mod \, 27$	m_i	MESSAGE
M	12	$20 \cdot 12 + 10 = 250 = 7 \, mod \, 27$	7	H
X	24	$20(24 - 13) = 20 \cdot 11 = 4 \, mod \, 27$	4	E
U	21	$20(21 - 13) = 160 = 25 \, mod \, 27$	25	Y
M	12	$20 \cdot 12 + 10 = 250 = 7 \, mod \, 27$	7	H
H	7	$20 \cdot 7 + 10 = 150 = 15 \, mod \, 27$	15	O
W	23	$20(23 - 13) = 200 = 11 \, mod \, 27$	11	L
X	24	$20(24 - 13) = 20 \cdot 11 = 4 \, mod \, 27$	4	E
Ñ	14	$20(14 - 13) = 20 \, mod \, 27$	20	T
R	18	$20(18 - 13) = 100 = 19 \, mod \, 27$	19	S
P	16	$20(16 - 13) = 60 = 6 \, mod \, 27$	6	G
H	7	$20 \cdot 7 + 10 = 150 = 15 \, mod \, 27$	15	O

EXERCISES

Exercise 1 Cipher via affine substitution, with key $(2,5)$ and the Spanish 27-letter alphabet (including ñ, and without blank spaces) the message AGENTE SECRETO (Spanish for SECRET AGENT).

Exercise 2 Decipher the message HW NEOYQ JSYR, which has been ciphered via affine substitution with key $(5,4)$ and the standard 26-letter English alphabet.

Exercise 3 Decipher the message PURTFJUIE LNPNPKNÑFLF, ciphered through affine substitution with key $(2,5)$ and the Spanish 27-letter alphabet.

Exercise 4 A hacker intercepts the following message: OSWGMSSONCIO. Through frequency analysis, the hacker has managed to deduce that letters G and N can be deciphered by U and P, respectively. Knowing that the alphabet in use is the standard 26-letter English alphabet, and that affine substitution is used, help the hacker decipher the message.

Exercise 5 Cipher the phrase ESTOY CIFRANDO CON VIGÉNERE (Spanish for I'M CIPHERING THROUGH VIGÉNERE) through Vigénere's cipher using the standard 26-letter English alphabet and the following key: $k = \{7,11,20,24\}$

Exercise 6 Given prime numbers $p = 163$, $q = 271$; and public key $K_P = (e,n) = (25277,163 \cdot 271)$, decipher the following messages:

a) 8767 **b)** 18582 **c)** 39760

Exercise 7 (February 2007) Users A and B want to start a secure session to share a large amount of data. To that extent, they are using the following hybrid cipher system: B will send A session key (a, b) to cipher data through a symmetrical algorithm. To send this session key, they will use RSA and the public key of A. When both know the session key, they will cipher and decipher their messages through affine substitution and the Spanish 27-letter alphabet.

a) A is a somewhat careless user and has used public key $K_P = (7,33)$. Find A's private key by using Fermat's method in the factorization of n.

b) B has sent the session key to A, but as an attacker, you have intercepted the cryptogram, finding that the first value is 29 and that the second value is 14. Decipher the session key and the message that A sent B to confirm the reception of the key: TEPFON.

Exercise 8 Users A and B want to start a secure session to share a large amount of data. To that extent, they are using the following hybrid cipher system: B will send A session key (a, b, c) to cipher data through a symmetrical algorithm. To send this session key, they will use RSA and the public key of A. When both know the session key, they will cipher and decipher messages through Vigénere with the Spanish 27-letter alphabet.

a) A is a somewhat careless user and has used public key $K_P = (19,161)$. Find A's private key by using Fermat's method in the factorization of n.

b) B has sent the session key to A, but as an attacker, you have intercepted the cryptogram, discovering that the first value is 52, the second value is 1, and the third value is 72. Decipher the session key and the message that A sent B to confirm the reception of the key: ÑFVVHQ

Exercise 9 Users A and B want to start a secure session to share a large amount of data. To that extent, they are using the following hybrid cipher system: B will send A session key (a, b) to cipher data through affine substitution and the standard 26-letter English alphabet. To send this session key, they will use RSA and the public key of A.

a) A is a somewhat careless user and has used public key $K_P = (43,77)$. Find A's private key by using Fermat's method in the factorization of n.

b) B has sent the session key to A, but as an attacker, you have intercepted the cryptogram, discovering that the first value is 64 and that the second value is 38. Decipher the session key and the message that A sent B to confirm the reception of the key: LQIFZ

Note: the second message that A sent to B was CHRISTMAS

References

Alfred J. Menezes, Paul C. van Oorschot y Scott A. Vanstone. "Handbook of Applied Cryptography". CRC Press, 1996.

Herbert B. Enderton, "A mathematical introduction to logic". Elsevier, 2001.

Norman L. Biggs, "Discrete mathematics". Oxford University Press, 2002.

W. K. Grassmann and J.P. Tremblay, "Logic and discrete mathematics: a computer science perspective". Prentice Hall, 1996.