uc3m | Universidad Carlos III de Madrid

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | COMPUTER SECURITY LAB (COSEC) GROUP

FINAL EXAM

ORDINARY SITTING MAY 2014

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Final Exam – Ordinary Setting May 2014

Surname:
Name:
Reduced Group:
NIA:

MULTIPLE CHOICE QUESTIONS (1 point)

Each question has only one correct answer, to be marked with an X in the appropriate box. Each question is worth 0.1. Each question wrongly answered takes 0.025 from the grade. Unanswered questions are not considered.

1. **Mark the correct statement.**

   □ 7^{13} mod 13 = 1.
   □ 7^{13} mod 13 = 7.
   □ 7 is not a generator of Z_{13} .
   □ None of the three above is true.

2. **Consider known plaintext attacks and chosen plaintext attacks:**

   □ In both cases just the plaintext and the encryption algorithm are known.
   □ In chosen plaintext attacks the key is known.
   □ The encryption algorithm is only known in known plaintext attacks.
   □ In both cases the cryptanalyst has access to the ciphertext.

3. **The Kasiski method is used:**

   □ In the cryptanalysis of monoalphabetic substitution methods.
   □ In the cryptanalysis of polyalphabetic substitution methods.
   □ To complement the frequency analysis of monoalphabetic substitution methods.
   □ None of the three above is true.

4. **Consider the modes of operation of block ciphers:**

   □ In every mode each block is encrypted separately, with no dependency of other blocks.
   □ In ECB mode each encrypted block depends on the precedent encrypted block.
   □ In CBC mode the ciphertext that corresponds to a specific plaintext block depends on the precedent ciphertext block. Likewise, the block of plaintext that corresponds to a specific block of ciphertext depends on the precedent ciphertext block.
   □ In CFB mode an error in a bit of the cryptogram will affect a single block of the recovered plaintext.

5. **Consider a block cipher in CFB mode such that the plaintext is arranged in blocks of 16 bits and the cipher takes inputs of 48 bits. If a ciphertext block is received with an error, such error:**

   □ Affects 16 blocks of the corresponding plaintext.
   □ Affects 3 blocks of the corresponding plaintext.
   □ Affects 4 blocks of the corresponding plaintext.
   □ Affects 2 blocks of the corresponding plaintext.

6. Consider a cryptosystem composed of n users:

- □ If symmetric encryption is used then the total number of keys involved is 2n.
- □ If symmetric encryption is used then the number of keys managed by a user is 2n.
- □ If asymmetric encryption is used then the total number of keys involved is 2n.
- □ If asymmetric encryption is used then the total number of keys managed by a user is 2n.

7. Regarding asymmetric encryption we can state that:

- □ Diffie-Hellman key exchange allows the agreement of a symmetric key between two peers, by means of public communications.
- □ El Gamal encryption algorithm produces ciphertext blocks larger than the corresponding plaintext blocks.
- □ Diffie-Hellman key exchange cryptanalysis is based on solving the discrete logarithm problem.
- □ The previous three are all correct.

8. Regarding digital signatures, the non-repudiation service:

- □ Guarantees that the received data have been sent by an authorized entity.
- □ Protects against authorship deniability against third parties.
- □ Prevents from the unauthorized used of a resource.
- □ Protects against unauthorized access to information.

9. If information has been modified by unauthorized users then it has been affected in its ___________.

- □ Integrity.
- □ Availability.
- □ Validity.
- □ Confidentiality.

10. Mark the correct answer regarding RSA algorithm parameters.

a

p – prime number, (private, chosen)
$n = p^2$, (public, computed)
e, m.c.d. $(\Phi(n),e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
$d = e^{-1}$, [mod($\Phi(n)$)], (private, computed)

b

p, q – two prime numbers, (public, chosen)
$n = p \cdot q$, (private, computed)
e, m.c.d. $(\Phi(n),e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
$d = e^{-1}$, [mod($\Phi(n)$)], (private, computed)

c x

p, q – two prime numbers, (private, chosen)
$n = p \cdot q$, (public, computed)
e, m.c.d. $(\Phi(n),e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
$d = e^{-1}$, [mod($\Phi(n)$)], (private, computed)

d

p, q – two prime numbers, (private, chosen)
$n = p \cdot q$, (public, computed)
e, m.c.d. $(e,n) = 1$, $1 < e < \Phi(n)$, (public, chosen)
$d = e^{-1}$, (mod(n)], (private, computed)

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Final Exam – Ordinary Setting May 2014

Surname:

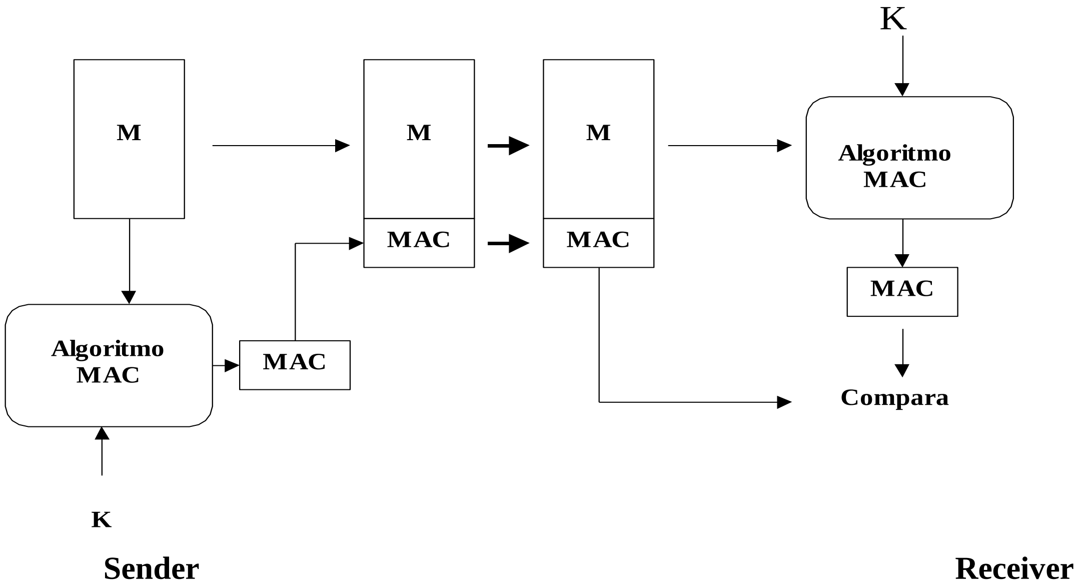
Name:

Reduced Group:

NIA:

QUESTION (0.5 points)

1. Explain message authentication with MAC functions by means of a block diagram.



The sender appends a Message Authentication Code (MAC) to the sent message M. Such MAC (a fixed length value) depends on a key K previously agreed between the sender and the receiver. The MAC algorithm is public and it is typically based on either a hash function (HMAC) or a symmetric block cipher (CBC-MAC). The receiver can check the integrity of the message computing the MAC from the received message M and the key K, and comparing it to the received MAC value. It is computationally unfeasible to find a message M' with the same MAC as

EXERCISE 1 (1.25 points)

Consider a PKI system that follows a hierarchical certification model such that:

- Each certificate authority has a unique numeric identifier.
- The certificate fields are expressed in decimal base and follow the format specified in the attached figure.
- The digital signature included in the certificates uses a scheme with hash function providing integrity to the remaning fields of the certificate. The signature algorithm is RSA with hash function H. H outputs a decimal digit and it works in two phases: 1.- It adds every field of the certificate in decimal base and 2.- It adds the decimal digits obtained in step 1, repeating this process until getting a single decimal digit (see the example below).
- Here you can find the certificate format (a simplification of X.509 certificates) and the corresponding description of each field.

FIELD	DESCRIPTION
ISSUER ID	Certificate issuer identifier
SUBJECT ID	Subject identifier
SERIAL NUMBER	Certificate serial number
ALG_ID	Signature algorithm identifier
e	RSA public key exponent
N	RSA public key modulus
DIGITAL SIGNATURE	Digital signature of the certificate

Consider the following information regarding the three Certificate Authorities involved in the system:

CA1 – Root Certificate Authority

CA1 certificate → C_{CA1} (1,1,0,1,5,91,34)

CA1 data corresponding to the certificate issue process:

Primes: p=7,q=13, RSA public key exponent: e=5

Output of the hash funtion H applied to the C_{CA1} fields:

1+1+0+1+5+91=99→ 9+9=18→ 1+8 =9 → $\mathbf{H_{AC1}= 9}$

CA2 – CA1 Subordinate Authority

Cert_CA2 → C_{CA2} (1,2,2,1,5,51,X)

CA2 data corresponding to the certificate issue process:

Primes: p=17,q=3

CA3 – CA2 Subordinate Authority

Cert_CA3 → C_{CA3} (2,3,4,1,5,21,Y)

1. Compute the certificate digital signatures (X and Y) of the subordinate authorities CA2 and CA3.

2. Consider a user that receives a certificate signed by CA3, and the corresponding certificates of the certificate chain. Consider that the user has just verified the signature of the certificate signed by CA3. Verify the certificates of the certificate chain and state if the user can trust the certificate signed by CA3. If she cannot trust, explain why and make the computations you need to solve(/mitigate) the problem . Explain if any further steps are neccesary to trust the received certificate.

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Final Exam – Ordinary Setting May 2014

Surname:

Name:

Reduced Group:

NIA:

SOLUTION:

1 X and Y computations

CA3

HASH: $2+3+4+1+5+21= 36 \rightarrow 3+6 = 9 \rightarrow$ **$H_{CA3}=9$**

HASH SIGNATURE:

d_{AC2} is not given but we can compute it from p,q and e

$p*q=n \rightarrow 17*3=51 \rightarrow n=51$

$\phi(n)=(p-1)*(q-1)=16*2=32 \rightarrow \phi(n)=32$

$e*d=1 \bmod 32 \rightarrow e=5 \rightarrow 5d=1 \bmod 32 \rightarrow$ **$d_{CA2}=13$**

$SRSA_{CA3} = H_{CA3}^{dCA2} \bmod n_{AC2} = 9^{13} \bmod 51=42 \rightarrow$ **$SRSA_{CA3}= 42 =Y$**

CA2

HASH: $1+2+2+1+5+51=62 \rightarrow 6+2=8 \rightarrow$ **$H_{CA2}=8$**

HASH SIGNATURE:

$p*q=n \rightarrow 7*13=91 \rightarrow n=91$

$\phi(n)=(p-1)*(q-1)=6*12=72 \rightarrow \phi(n)=72$

$e*d=1 \bmod 72 \rightarrow e=5 \rightarrow 5d=1 \bmod 72 \rightarrow$ **$d_{CA1}=29$**

$SRSA_{CA2} = H_{CA2}^{dCA1} \bmod n_{CA1} = 8^{29} \bmod 91=8 \rightarrow (8^4 \bmod 91 =1) \rightarrow (8^4)^7*8 \bmod 91 \rightarrow 1*8 \bmod 91=8 \bmod 91 \rightarrow$ **$SRSA_{AC2}= 8 =X$**

2. Certificate chain verification

First CA3 certificate is verified:

We compute **H_{CA3}** (already done before)

$H_{CA3}=9$

We encrypt the signature of CA3 certificate with CA2 public key(5,51):

$(SRSA_{CA3})^{eCA2}$ $\bmod n_{CA2} = 42^5 \bmod 51= (-9)^5 \bmod 51=9 =$ **H_{CA3}**

CA3 certificate is verified because the values match

Next, CA2 certificate is verified:

We compute **H_{CA2}** (already done before)

$H_{CA2}=8$

We encrypt the signature of CA2 certificate with CA1 public key (5,91):

$(SRSA_{CA2})^{eCA1}$ $\bmod n_{CA1} = 8^5 \bmod 91= 8 =$ **H_{CA2}**

CA2 certificate is verified because the values match

Next, CA1 certificate has to be verified. As it is a root certificate it is a self-signed certificate.

We compute the hash of the corresponding fields of the CA1 certificate

$H_{CA1}= 1+1+0+1+5+91=99 \rightarrow 9+9=18 \rightarrow 1+8=9$

$H_{AC1}=9$

We encrypt the signature of CA1 certificate with CA1 public key (5,91):

$(FRSA_{CA1})^{eCA1}$ $\bmod n_{CA1} = 34^5 \bmod 91= 34$

34 does not match 9. The verification fails and CA1 certificate is not valid. Therefore the certificate chain is invalid as well. In order to solve the problem, the signature has to be modified:

$SRSA_{AC1} = H_{CA1}{}^{dCA1} \bmod n_{CA1} = 9^{29} \bmod 91=81$
$(9^9)^3 * 9^2 \bmod 91 \rightarrow 81$
$SRSA_{CA1} = 81 \bmod 91$
The CA1 valid certificate would be C_{CA1} (1,1,0,1,5,91,81)

We can check the new signature: **($SRSA_{CA1}$)** $^{\mathbf{eCA1}}$ mod n_{CA1} = 81^5 mod 91=9 , that maches **H_{CA1}=9.**

The final step would be to follow a procedure to verify CA1's public key validity. Typically web browsers have root certificates embedded giving implicit trust to the corresponding public key. In addition a user should check if any of the certificates have been revoked before using it.

Table that summarizes computations

DATO	AC1	AC2	AC3
p	7	17	7
q	13	3	3
n	91	51	21
ϕ(n)	72	32	12
e	5	5	5
d	29	13	1
Hash Certificado	9	8	9
Firma sobre Hash	34 (81)	**8**	**42**

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Final Exam – Ordinary Setting May 2014

Surname:
Name:
Reduced Group:
NIA:

EXERCISE 2 (1.25 points)

A police inspector was in charge of solving the murder of Alice. Before the crime, two communications between the alleged murderer and the person who hired him were intercepted by the police. One was encrypted (C) while the other was not. The unencrypted communication was: “Boss, they will not catch us! Whenever I complete the job I will send you the first letter of the victim signed and encrypted using different algorithms. First I will sign it, with an algorithm that provides different signatures even if you sign the very same plaintext (I will use the first letter of the victim as output of the hash function). Then I will encrypt the first letter along with the obtained signature and I will send you the result. You know where to find my public keys; I have yours”. The inspector suspected the murderer did not use any standard to encrypt and sign, but he used the algorithms in a straightforward manner. Moreover, after inspecting the house of the alleged murderer, the forensic analysis of his computer revealed these data:

1. N=33, e=7
2. p=17, g=7, X=5, k=9

If the encrypted communication that was intercepted was C={C_1, C_2 ,C_3} = {0,10,20} and the alphabet used to code data was:

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

What were the encryption and signature algorithms used by the alleged murderer? What was the encrypted letter? Did the intercepted encrypted communication correspond to the data found in the computer of the alleged murderer? Why?

Solution:

From the intercepted communications and the forensic analysis of the computer, it can be concluded that for signing ElGamal signature algorithm was used, due to the fact that it is a randomized algorithm that generates different signatures from the same plaintext, according to a random parameter k. Therefore, the encryption algorithm was RSA (the exercise says that the signature and encryption algorithms are different, and the data found in the computer reveals it).

From the reading of the exercise we can conclude that:

C = Encryption$_{RSA}$(Signature$_{elGamal}$(M)) -> Signature$_{elGamal}$(M) = {M,r,s}

Decryption$_{RSA}$(C) = Signature$_{elGamal}$(M)

Boss' public key: e=7, N=33=p x q = 11 x 3

Boss' private key: fi(33)= 20, d= 3, ed mod fi(n) =1

Decryption$_{RSA}$(C_1) = 0^3 mod 33=0 -> 'A'

Decryption$_{RSA}$ (C_2) = 10^3 mod 33= 10 = r

Decryption$_{RSA}$(C_3) = 20^3 mod 33=14 = s

Therefore the decrypted message is {0,10,14} and the encrypted letter was letter 'A'. In order to know if the intercepted encrypted communication corresponded to the data found in the computer of the alleged murderer, the inspector can check if the signature is valid and created from the data found on the computer.

Y=7^5mod17=11

V1=11^10 x 10^14 mod 17=15 x 8mod17 =1

V2=7^0 mod17=1

Due to V1=V2 we can state that the alleged murderer is the real murderer (letter 'A' has been signed with the murderer's private key).

EXCERCISE MAKING OFF: C=Encryption$_{RSA}$(Signature$_{elGamal}$(M))={0, 10,20}

Signature$_{elGamal}$(M):

- H(M)= M= 0 ('A')
- r=7^9mod17=10
- 0=5 x r + 9 x smod16=5 x 10 + 9 x smod16 -> 14=9smod16
  - z=s/14 1=9zmod16->z=9
  - S=9 x 14mod16=14
- Signature$_{elGamal}$(H(M))={r,s}={0,10,14}
- {M,r,s}={0,10,14}

Encryption$_{RSA}$(Signature$_{elGamal}$(M)

- C1=0^7 mod 33=0
- C2=10^7 mod 33=10
- C3=14^7 mod 33=20
- C={0,10,20}