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 2013

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Final Exam – Ordinary Setting May 2013

Surname:
Name:
Reduced Group:
NIA:

MULTIPLE-CHOICE QUESTIONS (0,6 points)

Answer the following multiple-choice questions. Only one answer is correct.

1. **Let *a* be a primitive root (or generator) of Z_n, being *n* a non-prime number. Choose the correct answer:**
   a. There exists at least a power of *a* modulo n equal to 1.
   b. The order of *a* modulo *n* is $\Phi(n)$.
   c. The powers of *a* generate the reduced set of residues Z^*_n, that includes every element that has a multiplicative inverse in Z_n.
   d. a, b and c are all true.

2. **Mark which of the following answers is true:**
   a. The entropy of a source M measures the (a priori) uncertainty about the outcome before an observation of M.
   b. The entropy of a source M is the maximal information carried by a message that belongs to that source.
   c. The entropy tends to infinity when the source produces equiprobable messages.
   d. The lower the entropy is, the higher the uncertainty about the source M is.

3. **Mark which of the following statements is <u>NOT</u> true:**
   a. Block symmetric ciphers are typically slower than stream ciphers.
   b. Block symmetric ciphers are typically slower than asymmetric ciphers.
   c. Regarding the ciphers studied in class, stream ciphers are the fastest.
   d. Regarding the ciphers studied in class, asymmetric ciphers are the slowest.

4. **Mark which of the following sentences about Diffie-Hellman exchange protocol is true:**
   a. It allows to establish an encrypted and authenticated channel.
   b. It exchanges a secret between two parties, thus being susceptible to an interception attack.
   c. It allows to agree on a cryptographic key between two parties through an insecure channel, with no need to exchange any other secret previously.
   d. It is based on the ElGamal asymmetric scheme.

SHORT ANSWER QUESTIONS (0,40 puntos)

1. **Briefly explain an appropriate cryptosystem to exchange confidential and authenticated information from A to B (guaranteeing non repudiation by A). Consider that a great amount of information is transmitted from A to B. Briefly explain the strengths and weaknesses of the exposed system.**

2. **Build a scheme that classifies classic cryptographic methods on the one side and modern cryptographic methods on the other side. For each method, cite one or more examples.**

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Final Exam – Ordinary Setting May 2013

Surname:
Name:
Reduced Group:
NIA:

PROBLEM 1 (1,8 points)

The entity A wants to obtain a public key certificate from the Certificate Authority CA. The CA generates two key pairs, the former for signing (ElGamal signature algorithm with hash function Hash1) and the latter for encrypting (RSA algorithm). The CA uses its signature key pair to issue public key certificates for the CA users and for itself. The CA users use the CA encryption key pair to submit confidential requests to the CA.
The CA self-signs its own public keys to generate certificates that are available to CA users by means of a website. In addition, the CA also publishes the corresponding message digest of each certificate (in hexadecimal base), computed according to the hash function Hash2, in order to allow the users to verify the integrity of the certificates once downloaded.

Hash function specification and certificate format:

Hash1 is a function that accepts as input a list of elements codified in decimal base. Each of these elements are values in the interval [0,255]. The output of Hash1 is the result of computing the sum of every element of the list modulo 16. The output is codified in decimal.

Hash1 example: InputList = (35, 11). Hash1(35, 11) = (35 + 11) mod 16 = 14.

Hash2 is a function that accepts as input an ordered list of elements codified in decimal base. Each of these elements are values in the interval [0,255]. Hash2 codifies the input in binary and applies an i-bit right circular shift, where i is the position of the element in the list (first position = 1). The output of the function is the result of XORing every element after the shift. The result is codified in hexadecimal.

Hash2 example: InputList = (35, 11).
Hash2(35, 11) = RightCircShift [1]($00100011_{(2)}$) XOR RightCircShift[2]($00001011_{(2}$)= $01010011_{(2}$= $53_{(16}$

The certificates issued by the CA are composed of the following elements:

- identity of the user;
- elements of the user's public key;
- (r,s); the CA signature over the previous fields (ElGamal signature algorithm with hash function Hash1).

DATA:

Both A and the CA identities are codified as zero: $ID_{CA} = 0$, $ID_A = 0$.

CA signature parameters and keys: p = 17 (prime); g = 3 (generator); $X_{CA} = 4$ (private key);
$Y_{CA} = 13$ (public key)
$Cert_{CA}$-Sign = (ID_{CA}; Y_A; $S_{CA}(Hash1(ID_{CA},Y_A))$) = ($ID_{CA}$; Y_A; r, s) = (0; 13; 5, 5)

CA encryption keys: $n_{CA} = 33$ (modulus); $e_{CA} = 7$ (public exponent)
$Cert_{CA}$-Encrypt = (ID_{CA}; e_{CA}, n_{CA}; $S_{CA}(Hash1(ID_{CA}, e_{CA}, n_{CA}))$) = ($ID_{CA}$; e_{CA}, n_{CA}; r, s) = (0; 7, 33; 10, 0)

PART 1

A visits the CA web page and downloads both $Cert_{CA}$-Encrypt and $Cert_{CA}$-Sign (see DATA above). Published hash values for each of them are: $Hash2(Cert_{CA}\text{-Encrypt})=45_{(16}$ and $Hash2(Cert_{CA}\text{-Sign})=67_{(16}$

a) Compute how A verifies the integrity of the downloaded certificates by means of the published hashes in the CA website.
b) Compute how A verifies the validity of the $Cert_{CA}$-Sign.
c) Compute how A verifies the validity of the $Cert_{CA}$-Encrypt.

PART 2

A then generates a key pair for signature purposes (RSA algorithm with Hash1). A's public key is (e_A, n_A) = (5, 21). Afterwards, A generates a certificate request to be sent to the CA. Such request is A's signature over the data A wants to certify:

$$Request = (ID_A; e_A, n_A; S_A(Hash1(ID_A, e_A, n_A)))$$

Before sending it to the CA, A encrypts the request in order to make it confidential.

a) Compute d_A, A's private key.
b) Compute $S_A(Hash1(ID_A, e_A, n_A))$, the signature A generates from her identity and public key.
c) A must send to the CA the encrypted request. Indicate (do not perform the computations) how A would encrypt the request to the CA (if there is more than one element, consider that each element is encrypted independently).

PART 3

A sends to the CA the certificate generation request encrypted.

a) Indicate (do not perform the computations) how the CA would decrypt the encrypted request received from A.
b) Assume that, once decrypted, the request received by the CA is:

$$Request = (ID_A; e_A, n_A; S_A(Hash1(ID_A, e_A, n_A))) = (0; 5, 21; 19).$$

Make the computations the CA performs to verify the authenticity of the request received from A.
c) The CA proceeds to generate A's public key certificate. To this end it chooses k=7. Compute $Cert_A$ = (ID_A; e_A, n_A; $S_{CA}(Hash1(ID_A, e_A, n_A))$).

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Final Exam – Ordinary Setting May 2013

Surname:
Name:
Reduced Group:
NIA:

PROBLEM 2 (1,2 points)

Consider that Alice and Bob use a Vernam cipher to exchange confidential information. To produce the keystream they use a 4-cell LFSR with associated polynomial $f(x)= x^4+x^3+x^2+1$. In order to agree on the 4-bit seed ($K= a_1a_0b_1b_{0(2}$), Alice generates the 2 most significant bits of K ($K_A=a_1a_{0(2}$) and Bob the 2 least significant ($K_B = b_1b_{0(2}$). For the confidential exchange of the subkeys K_A and K_B, Alice and Bob decide to use RSA. Let K_A be $10_{(2}$, and consider that Alice receives from Bob the value $11000100_{(2}$. Take into account that Alice's public key is $(e_A, N_A)=(147, 253)$ and Bob's is $(e_B, N_B)=(7, 55)$.

a) Compute the value that Alice sends to Bob (express it in decimal base).
b) Compute K.
c) Ignore the previous result and let K be equal to $0110_{(2}$. Consider that the first ciphertext Alice receives from Bob is $C=3BC_{(16}$. Compute the corresponding plaintext Alice obtains, and express it in hexadecimal base.
d) Indicate if the keystream used has a maximum period or not. Justify your answer.

SOLUTION

PROBLEM 1 (1,5 points)

SOLUTION:

PART 1

a) Verification of $Cert_{AC}$-Sign

$Cert_{AC}$-Sign = (ID_{AC}; Y_A; S_{AC}(Hash1(ID_{AC}, Y_A))) = (0; 13; 5, 5)

Hash2($Cert_{AC}$-Sign) = RightCircShift[1]($00_{(16)}$) XOR RightCircShift[2]($0C_{(16)}$) XOR RightCircShift[3]($05_{(16)}$) XOR RightCircShift[4]($05_{(16)}$) = $67_{(16}$

0000 0000 → 0000 0000
0000 1101 1000 0110
0000 0101 0100 0001
0000 0101 1010 0000

0110 0111 = $67_{(16}$

$Cert_{AC}$-Encrypt = (ID_{AC}; e_{AC}, n_{AC}; S_{AC}(Hash1(ID_{AC}, e_{AC}, n_{AC}))) = (0; 7, 33; 10, 0)

Hash2($Cert_{AC}$-Encrypt) = RightCircShift[1]($00_{(16)}$) XOR RightCircShift[2]($07_{(16)}$) XOR RightCircShift[3]($21_{(16)}$) XOR RightCircShift[4]($0A_{(16)}$) XOR RightCircShift[5]($00_{(16)}$) = $55_{(16}$

0000 0000 → 0000 0000
0000 0111 1100 0001
0010 0001 0010 0100
0000 1010 1010 0000
0000 0000 0000 0000

0100 0101 = $45_{(16}$

Both hashes are the same as those published in the web page.

b) $Cert_{AC}$-Sign = (ID_{AC}; Y_A; S_{AC}(Hash1(ID_{AC}, Y_A))) = (ID_{AC}; Y_A; r, s) = (0; 13; 5, 5)

Hash1(ID_{AC}; Y_A)= 0 + 13 mod 16 = 13

$V_1 = Y_A^{\,r} \cdot r^{\,s} \bmod p = 13^{\,5} \cdot 5^{\,5} \bmod 17 = 371293 \cdot 3125 \bmod 17 = 13 \cdot 14 \bmod 17 = 182 \bmod 17 = 12$

$V_2 = g^{\,H(M)} \bmod p = 3^{\,13} \bmod 17 = 1594323 \bmod 17 = 12$

Cert is self-signed, so it is a root cert and there is no certification chain.

c) (ID_{AC}; e_{AC}, n_{AC}; S_{AC}(Hash1(ID_{AC}, e_{AC}, n_{AC}))) = (ID_{AC}; e_{AC}, n_{AC}; r, s)=(0; 7, 33; 10, 0)

Hash1(ID_{AC}; e_{AC}, n_{AC})= 0 + 7 + 33 mod 16 = 40 mod 16 = 8

$V_1 = Y_A^{\,r} \cdot r^{\,s} \bmod p = 13^{\,10} \cdot 10^{\,0} \bmod 17 = 16 \cdot 1 \bmod 17 = 16$

$V_2 = g^{\,H(M)} \bmod p = 3^{\,8} \bmod 17 = 6561 \bmod 17 = 16$

Cert is signed by AC but with other key pair; this verification has been done in the previous question.

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Final Exam – Ordinary Setting May 2013

Surname:
Name:
Reduced Group:
NIA:

PART 2

a) $e_A \cdot d_A \bmod \Phi(n_A) = 1$
$5 \cdot d_A \bmod \Phi(21) = 1$
$\Phi(21) = \Phi(3) \cdot \Phi(7) = 2 \cdot 6 = 12$
$d_A = 5$ ($5 \cdot 5 \bmod 12 = 25 \bmod 12 = 1$)

b) $Hash1(ID_A; e_A, n_A) = 0 + 5 + 21 \bmod 16 = 26 \bmod 16 = 10$
$S_A(Hash1(ID_A; e_A, n_A)) = H(M)^{dA} \bmod n_A = 10^{5} \bmod 21 = 19$

c) $Request = (ID_A; e_A, n_A; S_A(Hash1(ID_A, e_A, n_A))) = (0; 5, 21; 19)$.
A should encrypt each element in the request for AC:

$C(M_i) = M_i^{eAC} \bmod n_{AC} = M_i^{7} \bmod 33$

PART 3

a) $M_i = C(M_i)^{dAC} \bmod n_{AC} = C(M_i)^{dAC} \bmod 33$

$d_{AC} = 3$ (as $3 \cdot 7 \bmod 20 = 1$)

b) We retrieve the hash value from the signature:
$Hash1(ID_A; e_A, n_A) = S_A(Hash1(ID_A; e_A, n_A))^{eA} \bmod n_A = 19^{5} \bmod 21 = 10$
We also compute the hash value from received data:
$Hash1(ID_A; e_A, n_A) = 0 + 5 + 21 \bmod 16 = 26 \bmod 26 = 10$

They are the same, signatura is correct.

c) $r = g^{k} \bmod p = 3^{7} \bmod 17 = 11$

$s = (H(M) - X_A \cdot r) \cdot k^{-1} \bmod (p-1)$
$H(M) == Hash1(ID_A; e_A, n_A) = 10$ (computed in the previous question)
$k^{-1} \bmod (p-1) = 7^{-1} \bmod 16 = 7^{7} \bmod 16 = 7$
$s = (10 - 4 \cdot 11) \cdot 7 \bmod 16 = -34 \cdot 7 \bmod 16 = 14 \cdot 7 \bmod 16 = 2$

$Cert_A = (ID_A; e_A, n_A; S_{AC}(Hash1(ID_A, e_A, n_A))) = (0; 5, 21; 11, 2)$

Problem 2 (1,5 points)

Solution:
a)
$10_{(2} = 2_{(10}$
$2^7 \bmod 55 = 18$

b)
$11000100_{(2} = 196_{(10}$
Alice decrypts 196 with her private key
ed =1 mod fi(n)
147d =1 mod fi(253)

fi(253)= fi(11)fi(23)= 10*22= 220
147d = 1 mod 220
220 = 1*147 + 73
147 = 2*73 + 1

1= 147 – 2*73
1= 147 – 2*(220-147)
1= 147 – 2*220 + 2*147 = 3*147 – 2*220
d= 3

$196^3 \bmod 253$ =196*196*196-29761*253 =3
S = 1011

c)
0110
0<1100
1<1000
1<0001
0<0010
0<0101
0<1011
1<0110

The keystream has a period of 7. The sequence 0110001 is repeated

$3BC_{(16} = 0011\ 1011\ 1100_{(2}$
xor 0110 0010 1100
$0101\ 1001\ 0000_{(2} = 590_{(16}$

Alternatively

$3BC_{(16} = 0011\ 1011\ 1100_{(2}$
xor 0011 0100 0110
$0000\ 1111\ 1010 = 0FA_{(16}$

d) The period is 7 and it is not maximum because it is lower than 2^4 -1 = 15 that is the maximum period that can be produced by a 4-cell LFSR.