**Fınal Exam CMSE-512 10.06.2024, 16.30 (150 min, 100 points)**

St. Name, Surname\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Five A4-sized sheets of paper with your handwritten notes may be used. Calculators are allowed. Telephones and other electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 11 questions, 13 pages**

Good Luck!

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Task | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | Total |
| Point | 8 | 8 | 9 | 8 | 10 | 9 | 9 | 10 | 9 | 10 | 10 | 100 |
| Grade |  |  |  |  |  |  |  |  |  |  |  |  |

**Before MT Exam tasks 1-4 (33 points)**

**Task 1 (8 points)** Explaın why integrity is an ımportant security requırement

Integrity is an important security requirement because if unauthorized change is allowed, it can lead to very bad consequences, as in the case of the change of the route of an aircraft that can result in its crash.

**Task 2. (8 points)** What the salt is? How many bits does it take? What is the reason for keeping the ‘salt’ in the password file? (Fig. a)?



The ‘salt’ is a random or time-dependent value used for mixing with static passwords to introduce their variability. It takes 12 bits. The reason for keeping the salt in the password file is to have an ability to recalculate encrypted password from the password entered by a user and compare it versus the encrypted password stored in the password file.

**Task 3. (9 points)** Define an RSA private/public key pair if N=115. Show your calculations, give necessary explanations.

**Hints**: Two large prime numbers, *p* and *q*, , are selected, and an integer, *d*, is chosen that is relatively prime to *(p-1)(q-1)*. Finally, an integer e is computed such that

, N=pq, C=MemodN, M=CdmodN

EXTENDED EUCLID(m,b)

1. (A1,A2,A3):=(1,0,m); (B1,B2,B3):=(0,1,b);
2. if B3=0 return A3=gcd(m,b); no inverse
3. if B3=1 return B3 = gcd(m,b); B2= b-1 mod m
4. Q=
5. (T1,T2,T3):=(A1-QB1, A2-QB2, A3-QB3)
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

N=115=23\*5=p\*q, thus p=23, q=5

Fi(N)=(p-1)\*(q-1)=22\*4=88

E\*d=1 mod 88

Let e=3 then d=e^(-1) mod 88

Use EEA to find d:

A=(1,0,88), B=(0,1,3)

Q=floor(88/3)=29

T=A-q\*B=(1-29\*0,0-29\*1, 88-29\*3)=(1,-29,1)

A=B=(0,1,3)

B=T=(1,-29,1)

Since B3=1, then B2=-29 mod 88 = 59=d

Check it: e\*d=3\*59 = 177 = 2\*88+1 = 1 mod 88

Thus, e=3, d=59

**Task 4. (8 points)** Which bits of the 2nd round right half input R1 are defined by the outputs 1 and 2~~3~~ of the S-box S3 of the first round? Fill in the Answer table below. Explain your answer

**Hints**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |

|  |
| --- |
| Permutation function( P ) |
| 16 7 20 21 29 12 28 171 15 23 26 5 18 31 102 8 24 14 32 27 3 919 13 30 6 22 11 4 25 |

 |

Answer table:

|  |  |  |
| --- | --- | --- |
| Bit of R1 | S-box number | S-box output number |
| 24 | 3 | 1 |
| 16 | 3 | 2 |

Output bits 1 and 2 of S3 are bits number 9 and 10 after S-boxes’ outputs joined. According to the permutation P bit 9 goes to the position number 24 and bit 10 goes to position number 16.

**After MT Exam tasks 5-11 (67 points)**

**Task 5. (10 points)** Explain how the 64-bit registers *a,b,c,d,e,f,g,h* are initialized in SHA-512. Calculate the first three hexadecimal digits, 3c6, of the register *c*. Show your calculations, give explanations

**Hints**:





The registers are initialized as described here. For the register c, the 3rd prime, 5, is used

Sqrt(5)= 2.2360679774997896964091736687313

Multiply its fractional part by 16: 0.2360679774997896964091736687313\*16=3.7770876399966351425467786997004. Its integer part is 3 that is the 1st hexadecimal digit of c. Then the fractional part of the result again multiply by 16: 0.7770876399966351425467786997004\*16=12.433402239946162280748459195207 with 12 =C in the integer part of the result. Hence, the 2nd digit is C. And the fractional part again multiply by 16: 0.433402239946162280748459195207\*16=6.9344358391385964919753471233075 getting the 3rd digit 6 in the integer part of the result. Thus, the first three hexadecimal digits are obtained as 3c6.

**Task 6. (9 points)** What a certificate is, how many certificates are used in the SSL protocol, who and how generates them, how are they exchanged, and what for are they used?

**Hints:**

“Assume that a browser, C, connects to a server, S, that claims to represent a particular enterprise, E (for example, Macy’s). In this case, the protocol consists of the following steps:

1. S sends C a copy of its certificate signed by the CA – in the clear
2. C validates the certificate’s signature using the CA’s public key (included in its browser) and hence knows that the public key in the certificate belongs to the enterprise named in the certificate.
3. C generates and sends to S a session key encrypted with the public key in the certificate.”

The certificate is a document digitally signed by a certification authority (CA) certifying that some subject has some particular public key. One certificate of the Server is used in SSL. Certificates are generated by a CA as a readable text protected from tampering with by CA’s digital signature. The server sends his certificate to the client. Certificates are used to get trust to the public key mentioned in the certificate.

**Task 7. (9 points)** What are the actors of the SET protocol? What is the functionality of the Payment Gateway? What the dual signature is? How the dual signature is used by the Payment Gateway? Give detailed explanations.

**Hints:**

“Before SET begins, C and M negotiate the terms of a purchase. The protocol begins with a handshake in which C and M exchange certificates and authenticate each other. C sends its certificate to M, and M sends both its certificate and G’s certificate to C, at which point C and M know each other’s and G’s public key. Then the purchase transaction begins.

1. M sends a signed message to C containing a (unique) transaction Id (which is used to guard against replay attacks). C uses the public key in M’s certificate to check the signature and hence knows that the message came from M and was not altered in transit.
2. C sends a message to M containing two parts plus the dual signature:
3. The transaction Id, C’s credit card information, and the dollar amount of the order (but not a description of the items purchased) – encrypted with G’s public key:



1. The transaction Id, the dollar amount of the order, a description of the items purchased (but not C’s credit card information) – encrypted with M’s public key:



The dual signature has three fields:

1. The message digest, MD1, of the first part of the message:



where f is the message digest function

1. The message digest, MD2, of the second part of the message:



1. C’s signature of the concatenation of MD1 and MD2:



Thus, the complete dual signature is



and the complete message sent from C to M is .

The dual signature binds the two parts of the message. So, for example, an attempt by an intruder or M to associate  with  does not work since its message digest, MD2’, will differ from MD2. Although MD2’ can be substituted for MD2 in the dual signature,  cannot be used as the signature for MD1\*MD2’, and only C can compute the correct dual signature for the reconstructed message.

1. M decrypts the second part of the message with its private key (but it cannot decrypt the first part, which contains the credit card number). The merchant then
2. Uses the dual signature to verify that has not been altered in transit. It first computes the message digest of  and checks that it is the same as the second field of the digital signature (MD2). It then uses the public key in C’s certificate to check that the third field is the correct signature for the concatenation of the first two fields.
3. Verifies the transaction Id, the dollar amount of the order, and the description of the items purchased

Next M sends a message to G containing two parts:

(a)  and the dual signature it received from C:



1. The transaction Id and the dollar amount of the order – signed with M’s private and encrypted with G’s public key:



The complete message sent from M to G is , together with copies of C’s and M’s certificates

1. G decrypts the message using its private key.
2. It uses the dual\_signature and the public key in C’s certificate to verify that  was prepared by C and was not altered (as in step 3a).
3. It uses the message digest of the credit card information in C’s certificate to verify the credit card number supplied in .
4. It uses M’s signature in and the public key in M’s certificate to verify that  was not altered
5. It checks that the transaction Id and the dollar amount are the same in  and  (to verify that M and C agreed on the purchase)
6. It checks that the transaction Id was never submitted before (to prevent a replay attack)
7. It does whatever is necessary to approve the credit card request

Then G returns a signed approved message to M. At this point, the transaction is committed.

1. When M receives the approved message, it knows that the transaction has committed. It sends a signed message to C: transaction complete. C then knows that transaction has committed.”

The actors of SET protocol are: Client, Merchant, and Payment Gateway. The Payment Gateway is responsible for checking that Merchant and Customer both agree on the transaction with same particular ID number and amount of money, checks that the transaction ID is not repeated, checks validity of the Client credit card, debits Client’s credit card, and credits Merchant’s account. The dual signature is Client’s digital signature of the message digests of the messages m1 and m2 sent by Client to Merchant. The dual signature is used by Payment Gateway to check that m1 was prepared by Client and was not altered.

**Task 8. (10 points)** Given RSA public/private keys (5,91)/(29,91) and a valid serial number, $sn=12$, blind it, make a blinded token, and, un-blinding it,get a valid token, and check it validness assuming that the validity predicate is $valid(sn)= (sn mod 11 ==1)$.

Hints:

# “Creating a Blinding Function

The protocol requires that C creates his own blinding function, *b*, unknown to B. This might seem a difficult task, but it is actually quite easy in the context of RSA algorithm for public key cryptography. In one scheme for doing this, C first generates a random number, *u*, that is relatively prime to the modulus *N* of the bank’s keys. Because u is relatively prime to *N*, it has a multiplicative inverse, , with respect to *N*, such that



To blind the serial number, *n*, C computes



and sends the result to B. Hence, the blinding function can be viewed simply as multiplication by a random number.

The signed result, *sr*, returned by B to C is



Obviously, . To recover the token, we use



The serial number *n* can be now obtained using.”

Let $u=2, u^{-1} mod 91=46, b\left(sn\right)=E\_{P}\left(u\right)∙sn=2^{5}mod 91∙12 mod 91=32∙12 mod 91=32∙3∙4 mod 91=96∙4 mod 91=5∙4 mod 91=20$

$$sr=E\_{R}\left(b\left(sn\right)\right)=20^{29}mod 91= $$

$$20^{2} mod 91=20∙5∙4 mod 91=100∙4 mod 91=9∙4 mod 91=36$$

$$20^{4}=36^{2}mod 91=36∙36=36∙3∙12 mod 91=108∙12 mod 91=17∙12 mod 91=102∙2 mod 91=11∙2 mod 91=22$$

$$20^{8}=22∙22 mod 91=121∙4 mod 91=30∙4 mod 91=120 mod 91=29$$

$$20^{16}=29∙29 mod 91=841 mod 91=22$$

$$sr=20^{29}=20^{16}∙20^{8}∙20^{4}∙20 mod 91=22∙29∙22∙20 mod 91=29∙29∙20 mod 91=22∙20mod 91=110∙4 mod 91=19∙4 mod 91=76$$

$$sr=u∙token=2∙token=76$$

Hence, $token=38$. Decrypt token: $sn^{'}=38^{5}mod 91=$

$$38^{2}=19∙2∙19∙2 mod 91=76∙19 mod 91=-15∙19 mod 91=-3∙95 mod 91=-3∙4 mod 91=-12 mod 91=79$$

$$38^{4}=79∙79 mod 91=12∙12 mod 91=144 mod 91=53$$

$$38^{5} mod 91=38^{4}∙38 mod 91=53∙38 mod 91=53∙2∙19 mod 91=106∙19 mod 91=15∙19 mod 91=3∙95 mod 91=3∙4 mod 91=12=sn$$

Thus, we see that the decrypted token is our original serial sn=12, which valid since $sn mod 11=12 mod 11=1$.

**Task 9. (9 points)** What is the use of the tag ds:KeyInfo in the code below (Fig. 26.7)? What does it define in general? What does it define in that code in particular? What for is it used?

Figure 26.7. An encrypted element within an XML document

<PaymentInfo xmlns = “<http://...>”>

 <Name> John Doe </Name>

 <EncryptedData Type =

“

[http://www.w3.org/2001/04/xmlenc#Element”](http://www.w3.org/2001/04/xmlenc#Element\”  )

xmlns=”[http://www.w3.org/2001/04/xmlenc#](http://www.w3.org/2001/04/xmlenc)”/>

<EncryptionMethod Algorithm =

“[http://www.w3.org/2001/04/xmlenc#tripledes-cbc”/](http://www.w3.org/2001/04/xmlenc#tripledes-cbc)>

 <ds:KeyInfo xmlns:ds =

“[http://www.w3.org/2000/09/xmldsig#](http://www.w3.org/2000/09/xmldsig)“>

 <ds:KeyName>keyABC</ds:KeyName>

 </ds:KeyInfo>

 <CipherData>

 <CipherValue>Zx23XAbc4..</CipherValue>

 </CipherData>

 </EncryptedData>

</PaymentInfo>

The tag <ds:KeyInfo> is used in the code to refer to the secret key used. It defines in general what key is used for encryption/decryption. In particular, it defines the namespace [http://www.w3.org/2000/09/xmldsig#](http://www.w3.org/2000/09/xmldsig) and the key name as keyABC. It is used to specify what key is used in encryption/decryption.

**Task 10. (10 points)** Consider the two-way authentication procedure in Figure 14.5 below



**Answer the following seven questions a)-g); explain your answers.**

1. 1.5 points Who is authenticated to whom in way 1?

A is authenticated to B

1. 1.5 points Who is authenticated to whom in way 2?

B is authenticated to A

1. 1.5 points What is the meaning of A{x}?

It means that A digitally signs x

1. 1.5 points What is the meaning of tA, rA, IDB, sgndata, and EKUb[Kab] in the way 1 message?

tA, rA, IDB, sgndata, and EKUb[Kab] in the way 1 message mean respectively, timestamp, nonce generated by A, identifier of the receiver of the message, some data conveyed to the receiver protected from tampering with as covered by the signature of A, and protected from tampering with and from unauthorized reading session key Kab generated by A and encrypted by the public key of B

1. 1.5 points What for tA, rA are used in the way 1 message?

tA, rA are used in the way 1 message are used to counter replay attack

1. 1.5 points What parts of the way 1 message are protected from tampering with? Specify exactly names of the parts of the message

All the message parts are protected from tampering with as all of them are covered by A’s digital signature

1. 1 point What parts of the way 1 message are protected from unauthorized reading? Specify exactly names of the parts of the message

Kab is protected from unauthorized reading

**Task 11. (10 points)** What are the database administrator (DBA) responsibilities? How to protect a system from a dishonest system administrator? What is the system administrator default user name and password in the database management system you used in your Term project task?

DBA main responsibilities are 1) introducing new users to the system 2) monitoring the system performance; 3) upgrading the system resources when necessary. To protect the system from a dishonest DBA, it is recommended having at least two DBAs, so that if one is corrupted, another one can observe it.