**QUIZ2 CMSE-512 03.06.2024, 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, 10 pages**

Good Luck!

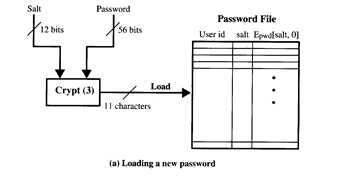
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Task | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | Total |
| Point | 8 | 8 | 9 | 8 | 10 | 9 | 9 | 10 | 9 | 10 | 10 | 100 |
| Grade |  |  |  |  |  |  |  |  |  |  |  |  |

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

**Task 1 (8 points)** Explaın why availability ıs an ımportant security requırement

Availability requirement is important for security since if a system is not available for operation there can be serious consequences as, e.g. if lung ventilation system goes out of operation the patient can die.

**Task 2. (8 points)** What are the two reasons of the ‘salt’ using when loading a new password in the UNIX password scheme (Fig. a)?



Reason 1: to have different effective passwords even if the users choose the same password

Reason 2: increase of the password key-space cardinality 4096 times thus making it more secure

**Task 3. (9 points)** Define an RSA private/public key pair if N=95. 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=95=p\*q=19\*5=>p=19, q=5

E\*d=1 mod (p-1)\*(q-1) =>e\*d =1 mod 72

Let e=5 then d is calculated by EEA:

A=(1,0,72), B=(0,1,5)

Q=floor(A3/B3)=floor(72/5)=14

T=A-q\*B= (1-14\*0, 0-14\*1, 72-14\*5) = (1, -14,2)

A=B=(0,1,5)

B=T=(1,-14,2)

Q=floor(A3/B3)=floor(5/2)=2

T=A-q\*B=(0-2\*1, 1-2\*(-14), 5-2\*2)=(-2,29,1)

A=B=(1,-14,2)

B=T=(-2,29,1)

Since B3=1, 5^(-1) mod 72 = B2 = 29=d

Check it: e\*d=5\*29 = 145 = 2\*72+1 = 1 mod 72. Let e be a public key, and d a private one.

**Task 4. (8 points)** What S-boxes and what their outputs of the 1st round of DES define the 4th and 5th bit values of the right half input R1 to the 2nd round? Fill in the Answer table below. Explain your answer

**Hints**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | |  | | --- | | Permutation function( P ) | | 16 7 20 21 29 12 28 17  1 15 23 26 5 18 31 10  2 8 24 14 32 27 3 9  19 13 30 6 22 11 4 25 | |

Answer table:

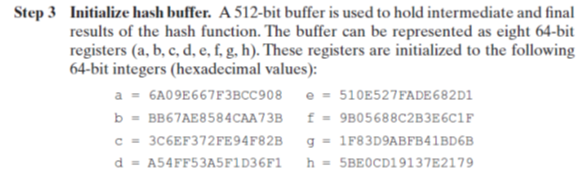
|  |  |  |
| --- | --- | --- |
| Bit of R1 | S-box number | S-box output number |
| 4 | 6 | 1 |
| 5 | 8 | 1 |

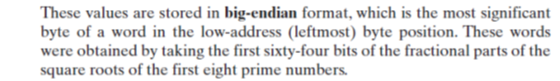
Bit 4 according to the P function is the bit 21 after S-boxes, hence, it is output 1 of S6. Bit 5 according to the P function is the bit 29 after S-boxes, hence, it is output 1 of S8.

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

**Task 5. (10 points)** Explain how 64-bit registers *a,b,c,d,e,f,g,h* are initialized in SHA-512. Calculate the 1st three hexadecimal digits, 6A0, of the register *a*. Show your calculations, give explanations

**Hints**:





In SHA-512, eight registers are initialized by 64 bits of the fractional parts of the square roots of the first eight prime numbers: 2,3,5,7,11,13,17, and 19.

Sqrt(2)= 1.4142135623730950488016887242097, its fractional part is 0.4142135623730950488016887242097. The first 16 digit is obtained by multiplication 0.4142135623730950488016887242097\*16=6.6274169979695207808270195873552, and taking its integer part, 6, as expected. Then again take the fractional part of the result and multiply by 16: 0.6274169979695207808270195873552\*16=10.038671967512332493232313397683, and take its integer part, 10=A, as expected. And, lastly, take the fractional part of the result, and multiply it by 16: 0.038671967512332493232313397683\*16=0.61875148019731989171701436292333. It integer part is 0 that is the 3rd hexadecimal digit: 6A0 as expected.

**Task 6. (9 points)** How many symmetric cryptography secret keys 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 actors are: Client and Server. Client initiates the protocol. Client generates the session key. Session key is protected from eavesdropping by encryption with the Server’s public key.

One symmetric key is created by Client. It is created somehow, may be, using random number generator. It is exchanged by sending encrypted with the public key of Server. It is used for further communication going encrypted by some symmetric cipher using the session key.

**Task 7. (9 points)** What is the dual signature used in SET protocol? What for is it used by the merchant, M? 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 dual signature is the digital signature generated by Client of the hash values of the two message parts sent by Client to Merchant, the first of them intended for the payment gateway, and the second for the Merchant. It is used by Merchant to validate his part of the message. And also Merchant forwards the dual signature to the payment gateway.

**Task 8. (10 points)** Let a cash serial number, *sn*, is represented as an unsigned 16-bit integer number with bits b15, b14,,,b1,b0. Its validity predicate, *valid(sn),* is defined so that it returns *true* if the sum of bits b8,..,b15 is greater than the sum of bits b0,.., b7, and *false*, otherwise. For example, sn=0xdcf1=1101110011110001 is not valid as having 5 bits both in the senior and junior halves. Write a C-like pseudocode to implement this predicate, *valid(sn).*

.

Int count\_bits(Byte val){

Int count=0;

For(i=1;i<=8;i++){

Count=count+val mod 2;

val=floor(val/2);

}

Return count;

}

Boolean Valid(sn){

Byte Junior= sn mod 256;

Byte Senior= floor(sn/256);

Bits\_sen=count\_bits(Senior);

Bits\_jun=count\_bits(Junior);

If Bits\_sen>Bits\_jun return True;

Else return False;

}

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

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 EncryptionMethod specifies a cipher used to encrypt the message content. Generally, it can be any symmetric cryptography method. In particular, 3DES is defined to be used in CBC (cipher block chaining) mode.

**Task 10. (10 points)** What for t1A, t2A, q1A, q2A are used in the simple Protected2 authentication? What attack can be mitigated with the help of these values? How this attack is conducted and how is it mitigated? Give necessary explanations



The timestamps, t1A, t2A, and nonces, q1A, q2A, are used as inputs to the hash function together with static user name and password. It is to counter replay attacks, when a previously sent message is resent, and it is necessary distinguishing between the first issue and the replay. For the first time, the message shall be accepted, for replays – rejected. Since timestamps and nonces uniquely define a particular message, if they repeat, it means replay attack is on. To recognize repetition, the server side shall maintain a database of the already received timestamps and nonces to compare versus the new ones. After acceptance, the timestamps and nonces used are stored in the database.

**Task 11. (10 points)** What are the database administrator (DBA) privileges? What DBA’s privileges can be granted to users? Give an example of SQL statement granting read access on the table Student to the user A with granting option

DBA privileges include new user introducing, granting him/her a new password, granting privileges to the users, managing system resources. DBA can grant a privilege of granting some privileges to the users. An example of such granting

Grant select on Student to A with grant option