**QUIZ2 CMSE-512 19.06.2023, 16.30 (150 min, 100 points)**

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

**SixA4-sized sheets of paper with your handwritten notes may be used. Calculators are allowed. Other electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 11 questions, 9 pages**

Good Luck!

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | T1 | T2 | T3 | T4 | T5 | T6 | T7 | T8 | T9 | T10 | T11 | Total |
| Point | 5 | 5 | 5 | 6 | 6 | 6 | 13 | 13 | 13 | 14 | 14 | 100 |

**Before MT Exam tasks 1-6 (33 points)**

**Task 1 (5 points)** What is the difference between the security threat and security vulnerability?

The security threat is the potential to violate a security requirement using a security vulnerability (weakness, breach, hole). The difference is that the security vulnerability is some, may be not disclosed yet, weakness in the software or hardware, but the threat is an opportunity to use it for breaking security.

**Task 2. (5 points)** What are the three methods to crack passwords?

1. Brute force attack. 2) stealing, 3) using spy software as key-loggers

**Task 3. (5 points)** Define an RSA private/public key pair if N=85. 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=85=p\*q, hence, p=17, q=5, fi(N)=(p-1)(q-1)=16\*4=64, Let e=3, then d= e^(-1) mod 64. Find it by EEA:

A=(1,0,64), B=(0,1,3)

Q=floor(A3/B3)=floor(64/3)=21

T=A-q\*B=(1-21\*0, 0-21\*1, 64-21\*3)=(1,-21, 1)

A=B=(0,1,3)

B=(1,-21,1)

Since B3=1, d=e^(-1) mod 64 = B2=-21 mod 64=43. Check it: 3\*43=129 mod 54 =1, that is OK

Hence, the public key is e=3, and the private key is d=49.

**Task 4. (6 points)** What S-boxes and what their outputs of the 1st round of DES define the 1st , 2nd, and 3rd 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 | |

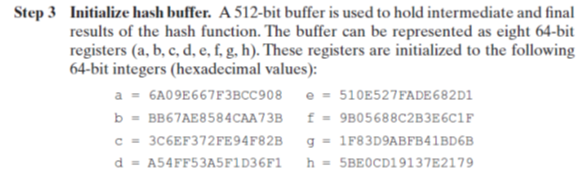
Answer table:

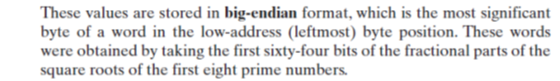
|  |  |  |
| --- | --- | --- |
| Bit of R1 | S-box number | S-box output number |
| 1 | 4 | 4 |
| 2 | 2 | 3 |
| 3 | 5 | 4 |

Explanation: The 1st bit of R2 is bit 16 after S-boxes according to P. Bit 16 is output by S4, output 4. Similar for others.

**Task 5. (6 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 (BB6) of the register *b*.

**Hints**:





For b initialization the prime 3 is used. Its square root is 1.7320508075688772935274463415059 with the fractional part 0.7320508075688772935274463415059. Multiplying it by 16 and taking the integer part of it, we get the 1st hexadecimal digit: b=11: 11.712812921102036696439141464094.

Taking the fractional part 0.712812921102036696439141464094 and again multiplying by 16 and taking its integer aprt, we get the 2nd hexadecimal digit b=11: 11.405006737632587143026263425503; Similar, for the 3rd digit, multiply 0.405006737632587143026263425503 by 16 getting 6: 6.4801078021213942884202148080532, as it was expected.

**Task 6. (6 points)** How many public/private keys are used in the SSL protocol, what is the type (private or public), and what for each of them is 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.

Two public keys are used. The 1st is the public key of the CA to validate the certificate. The 2nd is the server’s public key used to encrypt the session key generated by the client.

**After MT Exam tasks 7-11 (67 points)**

**Task 7. (13 points)** **What for** and **how** the payment gateway, G, uses the dual signature sent to it in SET protocol? 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 , where MD1, MD2 are hashes of the messages m1, m2, sent by C to M in the item 2 of SET. Merchant M sends in item 3 m1 and dual signature to G. G, knowing m1, can get its hash and compare versus MD1. Also, having MD1 and MD2,G can calculate f(MD1\*MD2) and compare it versus result of decryption of the 3rd component of the dual signature using the public key of C obtained from C’s certificate. If these checks successfully pass then G understands that actually M and C have agreed on the conditions of the purchase and can transfer money from C to M. Thus, it is done to make this decision.

**Task 8. (13 points)** What can be used as a serial number for the digital cash? How validness of a serial number is checked? What is the validity predicate? Define a validity predicate using each of the following arithmetic operations {+, -, \*}, and any one relational operator from {==, <=,<=, ~=}. Give an example of the valid and invalid serial number for the predicate you defined.

Any predicate can be used. Validness is checked by the predicate evaluation on a serial number. Validity predicate is any predicate taking a serial number as its input. Let validity(sn)=1- sn+sn\*sn<=15. Then validity(5)=1-5+25=21<=15 is false, then 5 is not a valid number. Validity(4)=1-4+16=13<=15 is true, hence, 4 is valid.

**Task 9. (13 points)** What is the meaning of the following XML code from the Lecture notes? What encryption algorithm is used in it by the sender? What key is used by the sender? What is encrypted? How it can be decrypted by the receiver? Give necessary explanations to your answers.

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>

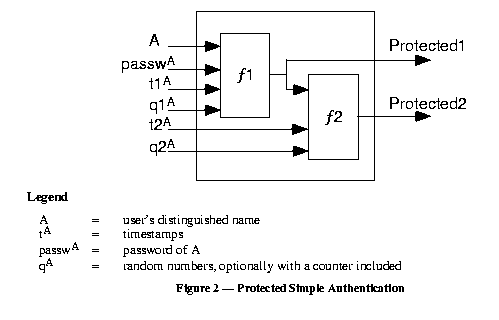
</CipherData>

</EncryptedData>

</PaymentInfo>

This is used to transfer payment information including sensitive data encrypted. Encryption algorithm used is 3DES in CBC mode.The key used is defined by its name, keyABC. Encrypted data is specified by the tag <CipherValue>, it cincerns sensitive payment data. It can be decrypted by applying 3DES-CBC with the key named keyABC fetched to the <CipherValue> provided in the code.

**Task 10. (14 points)** If A is using Protected2 from the figure below, explain how A can be authenticated by server B.



To be authenticated, A provides Protected2 together with A, passwA, t1A, q1A, t2A, q2A. The server, B, fetches A’s password from its database, and using the data provided, recalculates Protected2’ according to Fig. 2. If Protected2==Protected2’, A is authenticated.

**Task 11. (14 points)** What is a multilevel security database? How security attributes are incorporated into the relational database? What security levels are used? What two rules are used in the mandatory access control databases? What is the attribute security level? What is the tuple security level? Explain why the query

SELECT \* FROM EMPLOYEE.

output displayed is as shown below for user of the security level Confidential?

(a) Employee – the original tuples

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Salary | JobPerformance | TC |
| Smith U | 40000 C | Fair S | S |
| Brown C | 80000 S | Good C | S |

(b) Employee – after filtering for classification C users

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Salary | JobPerformance | TC |
| Smith U | 40000 C | NULL C | C |
| Brown C | NULL C | Good C | C |

A multilevel security database is such that uses Mandatory access control model. Security attributes are used in addition to information attributes: each information attribute is accompanied with the security attribute, and a tuple gets the tuple security label. Security levels mostly used are Top secret, Secret, Confidential, and Unclassified, with numerical equivalents, respectively, 3,2,1, and 0.The two rules used are “no read-up”, and “no write-down”. The attribute security level is defined by the value of respective security attribute in the tuple. The tuple security level is the maximum of the security levels of its attributes. The output is such because “no read-up” rule is applied precluding showing to the users of some level information of the higher levels (not shown data is shown as NULL with the user’s security level).