**Final Exam CMPE-552 13.01.2020 (120 min, 45 points)**

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

**Closed book. Calculators are allowed, other electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 8 questions (1-3, before MT, 15 points; 4-8, after MT, 30 points), 11 pages**

Good Luck!

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Total |
| 5 | 5 | 5 | 6 | 6 | 6 | 6 | 6 | 45 |
|  |  |  |  |  |  |  |  |  |

**Task 1. (5 points)** How memory protection is organized in multitasking operating systems? What is a virtual memory? What is difference between paged, segmented, and paged-segmented virtual memory organization? How system and user processes are distinguished?

Memory protection is made by allocating each process its own memory space. Virtual memory is a method using RAM memory together with external memory so that each process uses them as if it uses only RAM. In paged virtual memory, RAM and external memory are organized in same size pages. In segmented virtual memory, RAM and external memory are organized in generally different size segments. In segmented-paged virtual memory, different size segments are arranged as sets of same-sized pages. System and user processes are distinguished by different level privileges assigned to them.

**Task 2. (5 points)** Why password files shall be protected from unauthorized access?

What methods of password cracking do you know? What are three recommendations for passwords to be secure?

Password files shall be protected from unauthorized access because they contain sensitive data which may be used by malicious user for impersonation of authorized users. Methods of password cracking are, for example, brute force attacking, dictionary attacking. Three recommendations for passwords to be secure: use at least 8 symbols, use upper- and lower-case letters, use special symbols

**Task 3. (5 points)** Explain the difference between two kinds of malicious software: a Trojan horse and a virus.

The difference between a Trojan horse and virus is that a Trojan horse is intentionally invoked by a user not knowing about its undeclared functionalities, whereas a virus penetrates a user’s computer so that the owner of the computer does not know about it.

**Task 4. (6 points)** Let p=11, q=23. Specify RSA keys, encrypt and decrypt back the message M=10. Show your calculations. Give necessary explanations.

Hint:

RSA (Rivest-Shamir-Adelman, 1978) algorithm is an asymmetric encryption algorithm. To design an encryption/decryption key pair, two large prime numbers, p and q, , are selected, and an integer, d, is chosen that is relatively prime to (p-1)(q-1) (d and (p-1)(q-1) have no common factors other than 1). Finally, an integer e is computed such that



One key is (e,N), and the other is (d,N), where N=p\*q, and is referred to as the modulus.

For example, we might select p=7, and q=13. Then N=91, and (p-1)(q-1)=72. We can choose d=5 (which is relatively prime to 72) and e=29, because e\*d=145 and



Then, one key is K1=(29,91) and the other is K2=(5,91). The message to be encrypted is broken into blocks such that each block, M, can be treated as an integer between 0 and (N-1). To encrypt M into the ciphertext block, B, we perform



To decrypt B, we perform



The protocol works correctly because



More details about RSA algorithm can be found in the textbook by William Stallings, Cryptography and Network Security.

Returning to the example, assume M=2.

Then, to encrypt M, we compute



Thus, B=32. To decrypt B, we compute



which is the plaintext message M.

$$N=p∙q=11∙23=230+23=253$$

$$φ\left(N\right)=\left(p-1\right)∙\left(q-1\right)=10∙22=220$$

$e=3, d=e^{-1} mod φ\left(N\right)=3^{-1} mod 220$,

$$A=\left(1,0,220\right), B=(0,1,3)$$

$$Q=\left⌊A3/B3\right⌋=\left⌊220/3\right⌋=73$$

T=A-QB=(1,-73,1),

$$A=\left(0,1,3\right), B=(1,-73,1)$$

Since B3=1, $d=3^{-1} mod 220=B2= -73 mod 220=147$

Check it: $e∙d mod φ(N)=3∙147 mod 220=441 mod 220=2∙220+1 mod 220=1$

Encryption: $C=M^{e} mod N=10^{3} mod 253=1000 mod 253=3∙253+241mod 253=241=-12 mod 253$

Decryption: $M^{'}=241^{147} mod 253=(-12)^{147} mod 253= -12^{147} mod 253$

$$147=128+16+2+1$$

$$12^{147}=12^{128}∙12^{16}∙12^{2}∙12$$

$$12^{2} mod 253=144$$

$$12^{4} mod 253=144^{2} mod 253=144∙2∙72 mod 253=288∙72 mod 253=35∙72 mod 253=7∙5∙72 mod 253=7∙360 mod 253=7∙107 mod 253=749 mod 253=3∙253-10 mod 253= -10 mod 253=243$$

$$12^{8} mod 253=10^{2} mod 253=100$$

$$12^{16} mod 253=100^{2} mod 253=100∙4∙25 mod 253=400∙25 mod 253=147∙5∙5 mod 253= 735∙5 mod 253=\left(3∙253-24\right)∙5 mod 253=-24∙5 mod 253=-120 mod 253=133 $$

$$12^{32} mod 253=120^{2} mod 253=120∙2∙60 mod 253=240∙60 mod 253= -13∙60 mod 253= -780 mod 253=-3∙253-21 mod 253= -21 mod 253=232$$

$$12^{64} mod 253=21^{2} mod 253=441 mod 253=188 $$

$$12^{128} mod 253=188^{2} mod 253= 188∙2∙94 mod 253=376∙94 mod 253=123∙94 mod 253=123∙2∙47 mod 253=246∙47 mod 253= -7∙47 mod 253= -329 mod 253= -76 mod 253=177$$

$$12^{147}mod 253=12^{128}∙12^{16}∙12^{2}∙12 mod 253=\left(-76\right)∙\left(-120\right)∙144∙12mod 253=76∙6∙20∙144∙2∙6 mod 253=456∙20∙288∙6 mod 253=203∙35∙120 mod 253=203∙2∙60∙5∙7 mod 253=406∙300∙7 mod 253=153∙47∙7 mod 253= 51∙3∙7∙47 mod 253=357∙3∙47 mod 253=104∙3∙47 mod 253=312∙47 mod 253=59∙47 mod 253=2773 mod 253=243 mod 253= -10 mod 253 $$

M’=-12147 mod 253 = -(-10 mod 253) = 10=M

**Task 5. (6 points)** Using RSA keys from Task 4, digitally sign M=11 if the hash function is h(x)=3x mod 10. Specify what is sent by the signer to the receiver. As a receiver, validate the signature. Show your calculations. Give necessary explanations.

H(M)=3\*11 mod 10 = 33 mod 10 = 3

Signature= 3147 mod 253

34 mod 253 = 81 mod 253

38 mod 253 = 81\*3\*27 mod 253 = 243\*27 mod 253 = -10\*27 mod 253 = -270 mod 253 = -17 mod 253 = 236

316 mod 253 = 17\*17 mod 253 =289 mod 253 =36

332 mod 253 = 36\*9\*4 mod 253 = 324\*4 mod 253 = 71\*4 mod 253 = 284 mod 253 = 31

364 mod 253 = 31\*31 mod 253 = 961 mod 253 = 3\*253+202 mod 253 = 202 = - 51 mod 253

3128 mod 253 = 51\*51 mod 253 = 2601mod 253 = 71

Signature= 3147 mod 253 = 3128\*316\*32\*3 mod 253 = 71\*36\*9\*3 mod 253 = 71\*4\*81\*3 mod 253 = 284\*243 mod 253 = 31\*(-10) mod 253 = -310 mod 253 = -57 mod 253 = 196

Packet =(M, signature) = (11, 196)

Validation: Calculate H(M)=3\*11 mod 10 = 33 mod 10 = 3

Decryption of signature: 1963 mod 253 = 196\*196\*196 mod 253 = 196\*2\*98\*196 mod 253 = 392\*49\*392 mod 253 = 139\*49\*139 mod 253 = 139\*7\*7\*139 mod 253 = 973\*973 mod 253 = 214\*214 mod 253 = 39\*39 mod 253 = 39\*13\*3 mod 253 = 507\*3 mod 253 = 1\*3 = 3 that is equal to the original hash, hence the signature is valid

**Task 6. (6 points)** What for certificates are used in the SSL protocol? Who are the actors of the protocol? Who is expected having a certificate? How the certificate is validated? Who generates a session key? How the session key is hidden in transferring? How other party can unhide the session key? How the parties communicate after the session key is exchanged between them?

Certificates are used in SSL protocol to certify validity of a public key of the certificate owner. Actors of the protocol are a client and a server. A server is expected having a certificate. A certificate is validated by checking

* the digital signature of the certificate authority issued the certificate
* its validity period, and
* it is not revoked.

A session key is generated by the client. The session key is hidden in transferring by encrypting it with the public key of the server. The server un-hides the session key by decrypting it with its private key. The parties communicate, after the session key is exchanged, using it in some cipher.

**Task 7. (6 points)** Explain how the dual signature in the SET protocol is constructed. Who constructs it? What parts it has? What is the use of each part?

Hint: SET Protocol

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.

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.

A dual signature is constructed from the message digests, MD1, MD2, of the two parts, m1, m2, of the message sent by a customer to a merchant in the item 2 of the SET protocol. The dual signature binds MD1 and MD1 by a digital signature of their concatenation, i.e., the client encrypts with his/her private key, Rc, the result of hashing of the concatenation of MD1 and MD2. Thus, the dual signature is



The dual signature is constructed by a client. It has three parts: MD1, MD2, and the signature, ERc(f(MD1||MD2)).

MD1 together with the signature are used to validate m1 by the merchant the item 3 of SET.

MD2 together with the signature are used to validate m2 by the payment gateway in the item 4 of SET.

**Task 8. (6 points)** For the Anonymous cash protocol, using RSA settings of Task 4, get a valid token blindly signed by a bank. Assume that the redundancy predicate is valid(n)=(n2 mod 9=4). Specify other appropriate assumptions if necessary. Show your calculations. Give necessary explanations.

Hint:

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 n=2, then n2 mod 9 = 4. N=253, Pj=3, Rj=147.

Let u=5, u-1 mod 253 =?

A=(1,0,253), B=(0,1,5)

Q=floor(253/5)=50

T=A-Q\*B=(1,-50,3)

A=(0,1,5), B=(1,-50,3)

Q=floor(5/3)=1

T=A-Q\*B=(-1,51,2)

A=(1,-50,3), B=(-1,51,2)

Q=floor(3/2)=1

T=A-Q\*B=(2,-101,1)

A=(-1,51,2), B=(2,-101,1)

Thus, 5-1 mod 253 = -101 mod 253 = 152

Check it: 5\*152 mod 253 = 760 mod 253 = 3\*253 + 1 mod 253 = 1.

b(n)=EPj(u)\*n mod N = 53 mod 253 \* 2 mod 253 = 125\*2 mod 253 = 250 = -3 mod 253

sr=ERj(b(n))=(-3)147 mod 253 = -3147 mod 253 = |from Task 5|=-196 mod 253= 57.

Token = u-1\*sr mod N = 152\*57 mod 253 = 152\*3\*19 mod 253 = 456\*19 mod 253 = 203\*19 mod 253= -50\*19 mod 253 = -950 mod 253 = -(3\*253+191) mod 253 = -191 mod 253 = 62.

On the other hand, Token= 2147 mod 253 =62.

Actually,

28 mod 253 = 256 mod 253 = 3

216 mod 253 = 9

232 mod 253 = 81

264 mod 253 = 81\*9\*9 mod 253 = 729\*9 mod 253 = (3\*253-30)\*9 mod 253 = -30\*9 mod 253 = -270 mod 253 = -17 mod 253

2128 mod 253 = 172 mod 253 = 289 mod 253 = 36

2147 mod 253 = 2128\*216\*22\*2= 36\*9\*4\*2 mod 253 = 324\*8 mod 253 = 71\*8 mod 253 = 568 mod 253 = 2\*253+62 mod 253 = 62.