**QUIZ2 CMPE-552 27.12.2019 (120 min, 3 points)**

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

**Closed book, electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 8 questions (1-3, before MT, 1 point; 4-8, after MT, 2 points), 10 pages**

Good Luck!

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Total |
| 0.33 | 0.33 | 0.33 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 3 |
|  |  |  |  |  |  |  |  |  |

**Task 1. (0.33 points)** Why memory protection is important for providing security? Explain how a) confidentiality, b) integrity, and c) availability can be violated if memory protection is not provided.

Memory protection is important for providing security because contemporary operating systems allow several processes running concurrently in memory. Concurrently running processes can read information from the memory allocated for other processes thus violating confidentiality. Concurrently running processes can write into the memory of other allocated in the memory processes thus violating their integrity. Concurrently running processes can write into the memory of the other allocated in the memory processes thus disrupting their work and violating their availability.

**Task 2. (0.33 points)** What are the two ways of a password file protection from unauthorized access?

1 – restricting access to the file; 2 – using file encryption

**Task 3. (0.34 points)** Explain how “no write-down” rule can counter the Trojan horse attack.

Hint:



“No write-down” rule precludes writing by a high secrecy level process to a document of a lower level secrecy. Thus, if a high-level user invokes a Trojan horse malicious program that runs on the high level and has undeclared functionality such as writing into a file with low-level, when it reads a high-level secrecy document (see Fig. 15.10, c) and then tries writing it into low-level “back pocket” file for the further accessing it by a low-level user (see Fig. 15.10, d)), it is not allowed by the reference monitor.

**Task 4. (0.4 points)** Let p=13, q=19. Specify RSA keys, encrypt and decrypt back the message M=12. 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.

Apply Extended Euclid to find :

Check it:

Encryption:

.

Decryption:

**Task 5. (0.4 points)** Using RSA keys from Task 4, digitally sign M=122 if the hash function is h(x)=x mod 11. Specify what is sent by the signer to the receiver. As a receiver, validate the signature. Show your calculations. Give necessary explanations.

Digitally signed message is .

**Task 6. (0.4 points)** What for certificates are used? What three conditions a valid certificate shall meet?

Certificates are used to certify a public key of a subject. Three conditions are:

* Signature is valid
* Current date is inside the validness period
* The certificate is not revoked

**Task 7. (0.4 points)** What is the dual signature? Why SET uses the dual signature?

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.

The duals signature is



Where MD1, MD2 are message digests of messages m1, m2 sent by C, f is the hash function, Rc is the public key of C. SET uses dual signature to preclude changes made both in the parts intended to M and to G.

**Task 8. (0.4 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)=(n mod 11=2). 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.

The serial number, .

Find :

Thus,

Unblinded token is

On the other hand, token is 78.

Actually,

Token=.