**Final Exam CMPE-552 28.01.2022, 16.30 (120 min, 45 points)**

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

**Two A4-sized sheets of paper with your notes and a calculator may be used. Other electronic devices (telephones, laptops, etc.) are not allowed.**

Instructor Alexander Chefranov

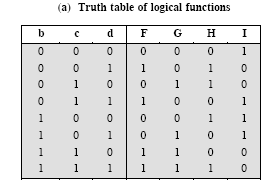
**Totally 5 questions (9 points each) + 6th bonus question (3 points), 8 pages**

**The maximal point might be earned is 45.**

Good Luck!

**Task 1. (9 points)** Prove that F(b,c,d) function used in MD5 actually can be represented as . Give necessary explanations

Hint:



Two functions are equal if their truth tables are the same. Calculate truth table of :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| b | c | d |  |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 |

Comparison of the truth tables for F in Table (a) and the calculated one shows that they are the same.

**Task 2. (9 points)** Explain who and why generates a session key in SSL protocol? Are certificates used in SSL? What the certificate is? What parts the certificate has?

Hint: 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.

Session key is generated by the client because only server has public key; it is used to encrypt the session key. Certificate is used to provide the public key of the server to the client. Certificate is an electronic document certifying public key of a subject by the digital signature of the certificate authority. Certificates has such parts as serial number, issuer, validity period, subject, public key of the subject.

**Task 3. (9 points)** For RSA with N=91, define private and public keys, and use them to generate a token from the valid (odd) serial number sn=3 by Anonymous digital cash protocol with blinding function based on RSA. Show you calculations. Provide necessary explanations.

**Hints:**

**Hint 1**: 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

**Hint 2**: 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.

N=p\*q=91=7\*13, p=7, q=13, fi(N)=(p-1)\*(q-1)=6\*12=72. Keys e, d meet e\*d=1 mod 72. If e=5 then d=29. Actually, e\*d=5\*29 = 145 mod 72 = 1. It can be found as

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(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=(-2,29,1)

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

Let public key PU=5, and private key PR=29

For blinding, u shall be selected such that gcd(u,N)=gcd(u,91)=1. Let u=5, then u^(-1) mod N = 5^(-1) mod 91 =

A=(1,0,91), B=(0,1,5)

Q=floor(91/5)=18

T=A-q\*B= (1-18\*0, 0-18\*1, 91-18\*5)= (1,-18, 1)

A=B=(0,1,5), B=T=(1,-18,1)

Since B3=1, 5^(-1) mod 91 = B2 = -18 mod 91 = 73

Let’s check it: 5\*73 = 365 = 4\*91+1 mod 91 = 1, hence, actually, 5^(-1) mod 91 =73.

B(sn)=E(PU,u)\*sn mod N = (5^5 mod 91 \* 3) mod 91 = 5^5\*3 mod 91 = 2.

Sr=E(PR,b(sn))=2^29 mod 91 = 32

Correct tag=u^(-1)\*sr mod N = 73\*32 mod 91 = 61

If the serial number sn=3 would be directly encrypted by PR, then tag1=3^29 mod 91 = 61. Thus, tag1=tag=61.

.

**Task 4. (9 points)** Explain how Protected1 and Protected2 on the Fig. 2 below can be used for protected password authentication. Give necessary explanations.



Protected1 is sent to server together with A, t1A, q1A. Server using A fetches A’s password APW, and checks f1(A, APW, t1A, q1A) == Protected1. If true, A is authenticated, otherwise – rejected.

Protected2 is sent to server together with A, t1A, q1A, t2A, q2A. Server using A fetches A’s password APW, and checks f2(f1(A, APW, t1A, q1A), t2A, q2A) == Protected2. If true, A is authenticated, otherwise – rejected.

**Task 5. (9 points)** Explain under what conditions and how with the help of the sequence of statistical queries Q1 and Q2

Q1: SELECT COUNT(\*) FROM PERSON

WHERE <condition>

Q2: SELECT AVG(Income) FROM PERSON

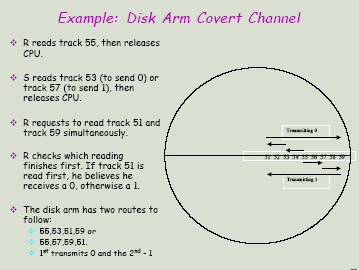
WHERE <condition>

it might be possible to reveal sensitive value of Income of the relation

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Name | Ssn | Income | Address | City | State | Zip | Sex | Last degree |

If the condition is defined so that the number of records meeting it is 1 (Q1 returns 1), then avg(Income) returned by Q2 will be an exact value corresponding to a person defined by the condition.

**Task 6. (3-point bonus)** Explain how illustrated by the figure below disk arm covert channel can be used to transfer binary data



Assume that disk controller serves first the nearest query in the direction of disk arm moving. If from track 55 set by R disk arm moved to track 53 (inward due to the request of S ), then, if after that two queries are issued by R (to 51 and 59), the 1st served will be 51 as closest in the current direction and response time for it will be less than that for track 59. Thus, it will be realized that S moved to 53 (transferred 0). Otherwise, S requested track 57, and 1 will be read out.