Homework 2: Your Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. (6) Consider a Diffie-Hellman scheme with a common prime *p=11* and a primitive root *g=2*.



1. If user A has a private key of 3, what is A’s public key?
2. If user B has a private key of 5, what is its public key?
3. What is their shared secret key K?

>>> Ya = 2^3 mod 11 = 8,

>>> Yb = 2^5 mod 11 = 10

>>> K = Ya^Xb mod 11 = 8 ^5 mod 11 = 10

1. (10 pts) Perform both encryption and decryption using the RSA algorithm for the following: (1) p=3, q=13, e=5, and M=3. (2) p=5, q=11, e=3, M=7; (you may guess d, you may use the repeated squaring based power reduction technique we introduced in the class)



**You must show at least the following details.**

1. **N = pq =39. Phi(n) = 2\*12 =24. ed =1 mod Phi (n) => 5d =1 mod 24 => d=5.**

**C = M^e mod n = 3^5 mod 39= 9.**

**M = C^d mod n = 9^5 mod 39 =3**

1. **N=pq = 55, Phi(n) = 4\*10 =40. ed =1 mod 40 => 3d =1 mod 40 => d =27.**

**C = M^e mod n = 7^3 mod 55= 13.**

**M = C^d mod n = 13^27 mod 55 = (13^2)^13 \* 13 mod 55 = 4^13 \*13 mod 55 = (4^3)^4 \* 4\*13 mod 55 = 9^4 \* 4\*13 mod 55 = 7**

1. (5 pts) In a public-key system using RSA, you intercept the ciphertext C=10 sent to a user whose public key is e=5, n=35. What is the plaintext M?



>>> n=35=5\*7, so phi(n) = 4\*6 =24. Because e \*d =1 mod phi(n), that is 5d =1 mod 24 -> d =5.

M = C^d mod n = 10^5 mod 35 = 5

1. (6pts) Let h1 and h2 be two hash functions. Show that if either h1 or h2 is collision resistant, then the hash function h(x) = h1(x) ||h2(x), is collision resistant. (here || means concatenation).

>>>Prove by contradiction: let us assume h1 is weak collision resistant (strong one is similar), it means that for a given x1 and h(x1), it is infeasible to find x2 != x1 such that h(x2) = h(x1). Now suppose h(x) = h1(x) ||h2(x) is not collision resistant. Then there exist x2 != x1, h(x2) = h(x1). That is, h1(x1) ||h2(x1) = h1(x2) ||h2(x2) => h1(x1) = h1(x2). This is a contradiction to our assumption.

1. (9 pts) Given that we have 46 students in our classroom, compute (1) what is the probability p1 that there is at least another people who have the same birthday as yours (2) what is the probability p2 that there are at least two people who have the same birthday? (3) based on the previous result, please explain why for SHA-1, its actual security strength is only about 80 bits.
2. **P1= 1 – (364/365)^45 =0.119**
3. **P2 = 1- (364/365)(363/365)(362/365)…(320/365) =0.94**
4. **Even with around sqrt(365) people, the probability of at least two people share the same birthday is close to 1. So the actual strength of SHA-1 is 160/2=80 bits.**
5. (8 pts) In this problem we will compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume that Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.
6. (Message integrity) Alice sends a message x = “Transfer $1000 to Mark” in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces “Mark” with “Oscar”. Will Bob detect this?
7. (Replay) Alice sends a message x = “Transfer $1000 to Oscar” in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?
8. (Sender Authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob but Alice claims the same. Can Bob clear the question in either case?
9. (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g. “Transfer $1000 from Alice to Bob.”) but Alice claims she has never sent it. Can Alice clear this question in either case?
10. With both DS and MAC, Bob will detect it.
11. Not for either case, because there is no clue to Bob x is replayed by Oscar or is multiple sequential transactions by Alice.
12. Yes. In the case of MAC, because Oscar does not know the symmetric key, it is impossible for him to generate valid auth(x) – it must be from Alice. DS is generated based on private key. With Alice’s public key, bob can verify it is from Alice or not.
13. In the case of MAC, no , because they both know the key. In the case of DS, yes.
14. (6 pts) What is a PKI? What are the three trust models for PKI (explain their meanings and example in some details)?

>>> Monopoly, Oligarchy, Anarchy models.

Additional problems from the textbooks:

4.2: (6 pts)

a. Nothing. It's a public key certificate, and public keys are public.

b. Hash the \message" and decrypt the signed quantity (using the CAs public key),

then compare the two.

c. Nothing. If Bob trusts the CA, he believes that the private key corresponding to

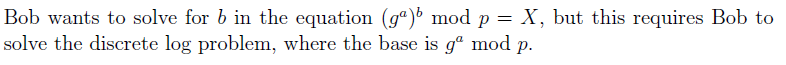
the public key in the certificate is held by Alice.

4.6. (8 pts)



4.12 (4pts) Encrypt the exchange.

4.13 (5pts)



5.4. (7 pts)

a. It is not precise but an estimation. Both solutions are correct.

(solution 1) Let the size of input be M= 1024=2^10, the output be N = 2^12. This is like you really throw M balls into N bins. The probability of a specific bin receives one ball is (M/N) and the probability to receive two balls is (M/N)^2 (i.e., a collision). There are totally N bins, so the total number of collision is N\* (M/N)^2 = M^2/N = 2^8.

(solution 2) The probability a pair of balls falling into a specific bin is p1=(1/N)^2, and the probability they fall into any same bin is p2= p1\*N = 1/N (i.e. a collision). They are totally 2 out of M (2-combination) pairs of balls, so the total number of collisions will be 1/N\*M\*(M-1)/2.

b. M^2/2^n. (corresponding to solution 1). (n: bits output; m: message bits;)

5.17. (8 pts)



5.21 (6 pts)



5.30 (6 pts)

