

**Student Name:** \_\_\_\_\_

**Student ID:** \_\_\_\_\_

## CS 134 FINAL

### Problem 1

---

Mark TRUE or FALSE for each statement:

- 1    **T**   **F**   Security through obscurity refers to the practice of obscuring a user's password when the user types it in, so that no one else can see it on the screen.
- 2    **T**   **F**   Deferring/delaying messages between two parties is considered a passive attack.
- 3    **T**   **F**   Caesar cipher is a particular version of the Affine cipher.
- 4    **T**   **F**   The costliest operation in DES is modular multiplication.
- 5    **T**   **F**   The natural logarithm (log base e) is a good hash function.
- 6    **T**   **F**   A hash function  $H()$  is said to be (weakly) collision resistant if for any  $x$ , it is computationally infeasible to find  $y$  such that  $H(y) = H(x)$  and  $y \neq x$ .
- 7    **T**   **F**   A group  $(G, @)$  is said to be ABELIAN if for all  $x, y, z$  in  $G$ :  $(x @ y) @ z = x @ (y @ z)$ .
- 8    **T**   **F**   In a Public Key cryptosystem, if Alice wants to send Bob an encrypted message, she has to generate a public/private key pair.
- 9    **T**   **F**   Public Key cryptography can be used to provide non-repudiation of origin.
- 10   **T**   **F**   CRLs are used in implicit certificate revocation systems.

### Problem 2

---

What is the minimum number of people we need to randomly pick so that the probability is 90% of at least two of them have the same birthday?

**Student Name:** \_\_\_\_\_

**Student ID:** \_\_\_\_\_

Problem 3

---

You are given a ciphertext  $C$  which was encrypted with some known RSA public key  $(e, n)$ . Also, suppose that you know that the plaintext has a common factor with  $n$  (but you don't know that common factor).

Can you discover the plaintext? the private key? the factorization of  $n$ ?

Problem 4

---

Suppose that Alice is using the El Gamal signature scheme. She signs two messages,  $m_1$  and  $m_2$ , but she uses the same random number  $r$  in each signature. Explain what danger stems from this.

Here's how the El Gamal Signature Scheme works:

$p$  – large prime

$b$  – base, generator

$x$  – private exponent

$y$  – public residue;  $y \equiv b^x \pmod{p}$

$P = Z_p^*$

$A = Z_p^* \times Z_p^*$

publics :  $p, b, y$

secrets :  $x$

Signing :

1. generate random  $r \in Z_{p-1}$

2. compute :  $k = b^r \pmod{p}$

3. compute :  $c = (m - xk)r^{-1} \pmod{p-1}$

4. signature =  $\{k, c\}$

Verifying :

$y^k k^c \pmod{p} = b^m \pmod{p}$  ???

notice that :

$y^k k^c = b^{xb^r} (b^r)^{(m/r - xk/r)} = b^{xb^r + m - xb^r} = b^m$

**Student Name:** \_\_\_\_\_

**Student ID:** \_\_\_\_\_

Problem 5

---

In authentication protocols, the following 3 types of quantities are used:

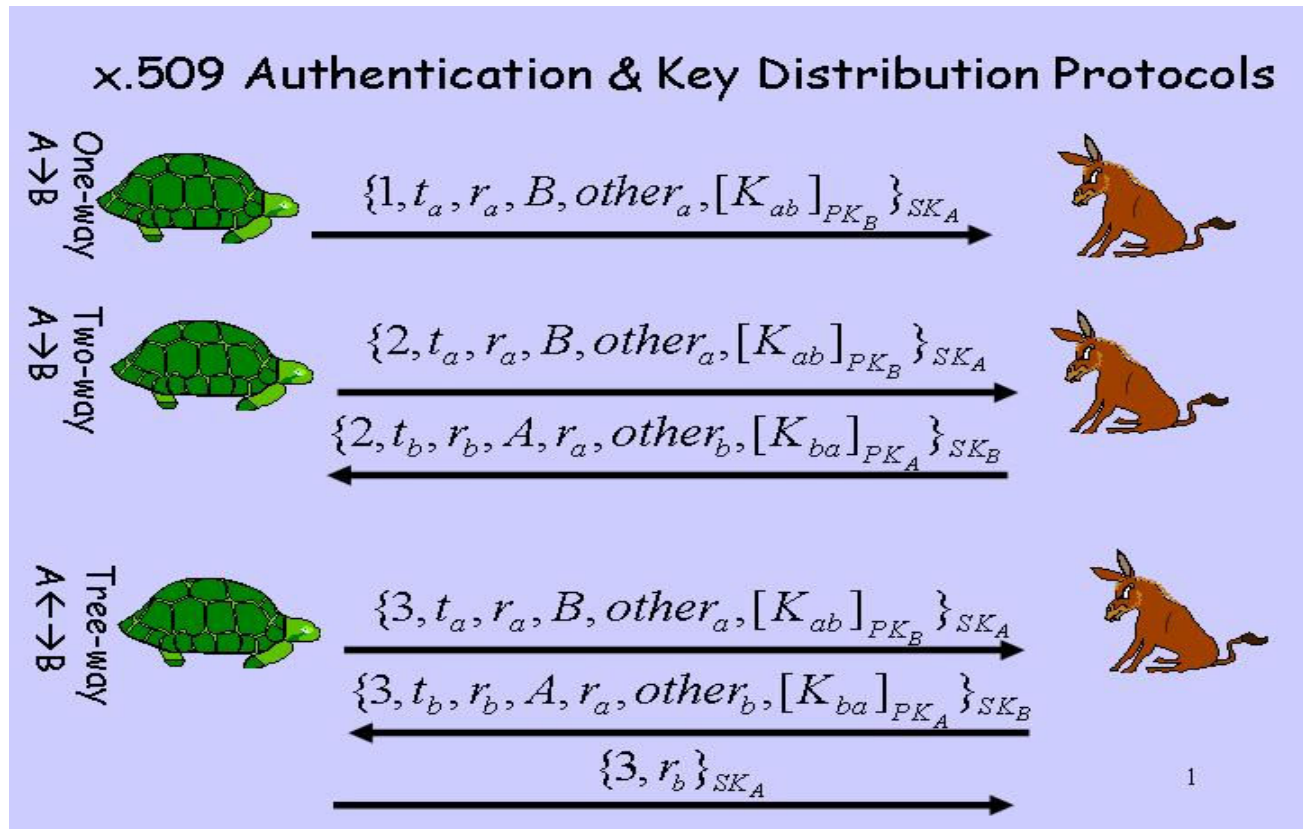
- a) Large random numbers (nonces or challenges)
- b) Timestamps
- c) Sequence numbers

Describe the advantages/disadvantages associated with using each of them.

Student Name: \_\_\_\_\_

Student ID: \_\_\_\_\_

Problem 6



- A) What will happen if we delete  $t_a$  from the 1<sup>st</sup> message in the 2<sup>nd</sup> protocol?
- B) What will happen if we delete A's name from the 2<sup>nd</sup> message in the 2<sup>nd</sup> protocol?
- C) What if we get rid of  $r_a$  in the 1<sup>st</sup> protocol?

**Student Name:** \_\_\_\_\_

**Student ID:** \_\_\_\_\_

Problem 7

---

Briefly describe any TWO of the following revocation methods:

- a) CRL
- b) CRT
- c) CRS
- d) OCSP

Problem 8

---

- a) How can a certificate owner "commit suicide" if s/he thinks that his/her private key has been compromised?
- b) Why do we remove expired certificates from CRL lists?
- c) If a certificate serial number is not on a CRL list, does this guarantee that it has not been revoked?

**Student Name:** \_\_\_\_\_

**Student ID:** \_\_\_\_\_