

CS 427/527 Midterm Review

1. What is the difference between cryptography and cryptanalysis?
2. Be able to define the following terms:
 - a. Confidentiality - Services to keep information secret during processing, transmission and/or storage.
 - b. Integrity - Service to protect the accuracy of stored or transmitted information with the capability to detect any alteration.
 - c. Authentication - Service to reliably validate the identity of others (e.g., systems or users).
 - d. Availability - Service to ensure systems are available to legitimate users.
 - e. Non-Repudiation - Service to eliminate plausible deniability - senders/receivers cannot deny having sent/received a message.
3. Know the basic assumptions about the cryptographic environment: (e.g. adversary has access to cipher text).
4. What is the difference between unconditional security and computational security?
5. What is steganography?
6. What is the Caesar cipher?
7. What is the Playfair cipher:
 - a. Maps letters into a 5 x 5 matrix (Z is omitted) and
 - b. follows three rules.
 - i. Arrange plaintext into pairs. If a double letter (e.g., tt) insert an X. If an odd number, insert an X pad at the end.
 1. If pair is in same row, cipher pair is two letters to the right wrapped to left column.
 2. If pair is in same column, cipher pair is below, wrap to top.
 3. If pair is at corners of a rectangle of letters, 1st encrypts to corner of same row, 2nd to corner in its row.
8. How do you unconditionally secure a Vigenere cipher? What is this cipher known as?
9. Know the characteristics of DES
 - a. Fixed block size in, fixed block size out. For DES a block = 64-bit plaintext/64-bit ciphertext out.
 - b. Fixed/variable key length.
 - c. DES key length = 56-bit, input as a 64-bit value, where every 8th bit is parity on the preceding 7 bits – used to check for key errors. This key is called the initial key.
 - d. Initial keys are used to generate sub-keys (round keys). DES initial key is used to generate 16 sub-keys, each 48 bits long.
10. Known how to use an expansion/permutation array.
11. Know how to use a S-Box from simple-DES.
12. Describe Cipher Block Chaining (CBC) Mode.
 - a. Chaining adds a feedback mechanism to a block cipher. With feedback, the encryption of the current block depends on the plaintext, key, and the previous block. For the first block an Initializing Value (IV) is used. Two

identical plaintexts encrypted under the same key don't produce the same output (unlike ECB). That is:

$$C_i = E_k(P_i \oplus C_{i-1})$$

$$P_i = C_{i-1} \oplus D_k(C_i) \text{ where } i = \text{block number}$$

13. Know basic modular arithmetic (addition, multiplication, GCD).

14. Know the Euclidean Algorithm to compute GCD(a,b) is:

EUCLID(a,b)

if(b==0) return a;

return Euclid(a, a mod b)

15. Know the extended Euclidean Algorithm

Extended-Euclid(a,b)

Input: two positive integers

Output: Integers x, y, d such that $d = \gcd(a,b)$ and $ax+by = d$

if $b=0$: return (1,0,a)

$(x',y',d) = \text{Extended-Euclid}(b, a \bmod b)$

return $(y', x' - \text{floor}(a/b) y', d)$

16. Know how to perform polynomial arithmetic in a Galois Field. (Most likely there will be a simple problem involving multiplication or division in a Galois Field).

17. Know definitions for prime and relatively prime.

18. Know Fermat's Little Theorem.

19. Know Euler's Totient Function.

20. Know Euler's Theorem.

21. Know the RSA Algorithm. (There will be a problem on the test).

22. Know how to compute large numbers mod n:

23. Example: For $3^{43} \bmod 13$:

$$3^1 \bmod 13 = 3 \bmod 13 = 3$$

$$3^2 \bmod 13 = 9 \bmod 13 = 9$$

$$3^4 \bmod 13 = 9^2 \bmod 13 = 81 \bmod 13 = 3$$

$$3^8 \bmod 13 = (3^4)^2 \bmod 13 = 3^2 \bmod 13 = 9$$

$$3^{16} \bmod 13 = (3^8)^2 \bmod 13 = 9^2 \bmod 13 = 81 \bmod 13 = 3$$

$$3^{32} \bmod 13 = (3^{16})^2 \bmod 13 = 3^2 \bmod 13 = 9$$

$$\text{So... } 3^{43} \bmod 13 = (3^{32} \times 3^8 \times 3^2 \times 3^1) \bmod 13$$

$$= (9 \times 9 \times 9 \times 3) \bmod 13 = 2187 \bmod 13 = 3$$

24. Know what a primitive root is.

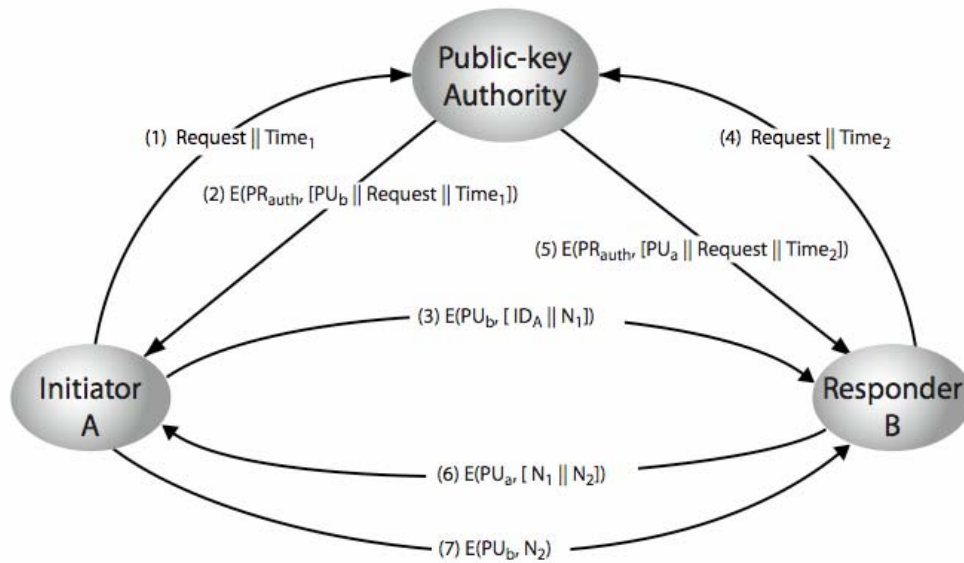
25. Know Discrete Logarithms.

a. The inverse problem to exponentiation is to find the **discrete logarithm** of a number modulo p that is to find x such that $y = gx \pmod{p}$ this is written as $x = \log_g y \pmod{p}$ if g is a primitive root then it always exists, otherwise it may not, eg.

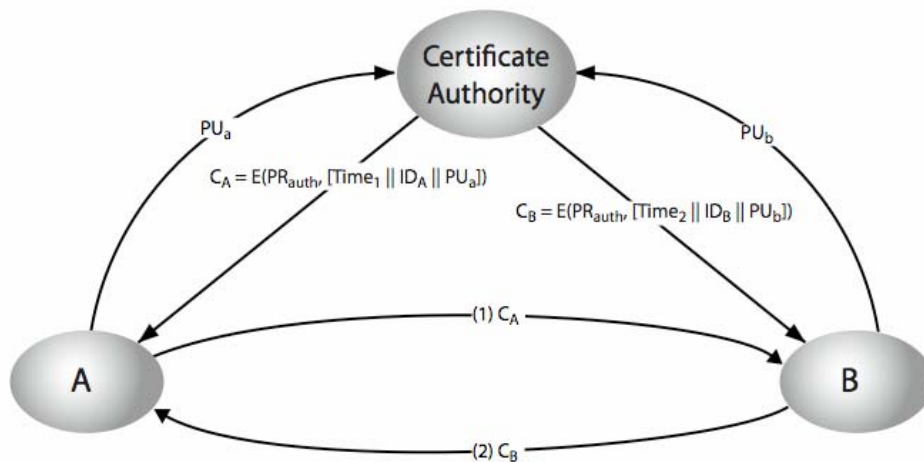
b. whilst exponentiation is relatively easy, finding discrete logarithms is generally a **hard** problem

26. Know the Diffie-Hellman key exchange algorithm

27. Know the public key authority approach to key management and why it's used:



28. Know the certificate authority approach to key management.



29. What is the benefit of the certificate approach?

30. What is the man in the middle attack?