1. (a) Consider You are designing a encryption scheme. Let say, the Message space is $\mathcal{M}$. What are the standard algorithms/components that you must have to define for your scheme. Explain these components. Explain their possible nature (Like whether they are probabilistic or deterministic) in case of perfectly secret private key encryption scheme.

   (b) Give formal specifications of the above mentioned components for at least two historical cipher. Make proper assumptions if needed.

2. (a) Explain Shift cipher and the Vigenere cipher in brief. Show how to use the Vigenere cipher for encryption of a word of length l. Is it possible to achieve perfect secrecy using Vigenere cipher in the above encryption? (you can make proper assumption about the key.) Prove your answer. Briefly Explain how someone can break Shift and Vigenere ciphers? Is there any case when Vigenere cipher is perfectly secret? Explain your answer.

   (b) Consider the Vigenere cipher over the lowercase English alphabet, where the key length can be anything from 8 to 12 characters. What is the size of the key space for this scheme?

   (c) Can you perform some modification in the standard version of Vigenere Cipher using the approach explained below? Is the Modified version completely secure, or can you break this Modified version? Justify your answer.
   Approach: For the Modified version of Vigenere cipher, one approach would be to Consider using multiple mono-alphabetic substitution ciphers, instead of using multiple shift ciphers. That is, the key consists of t random permutations of the alphabet, and the plaintext characters in positions i; t + i; 2t + i and so on are encrypted using the ith permutation.

3. Show that Shift, Substitution, Vigenere Ciphers are all trivial to break using a known-plaintext attack. (Assume only normal English words are being encrypted in each case.) how much known plaintext is needed to completely recover the key for each of the ciphers (without resorting to any statistics)?

4. Perfect Secrecy

(a) Prove or refute: Every encryption scheme for which the size of the key space is equal to the size of the message space, and for which key are chosen uniformly from the key space, is perfectly secret.

(b) Prove or refute: Consider a scheme for shift cipher where only a single character is encrypted.This scheme is perfectly secret.

(c) Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$ every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$

$$\Pr[M = m|C = c] = \Pr[M = m'|C = c]$$

(d) Prove or refute: One time pad is a perfectly-secret encryption scheme.

(e) What is the largest plaintext space $\mathcal{M}$ you can find for which the mono-alphabetic substitution cipher provides perfect secrecy? (Note: $\mathcal{M}$ need not contain only valid English words.)

5. (a) Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50 percent probability. Say the distribution over plain texts is Pr[M='aa'] = 0.4 and Pr[M='ab'] = 0.6. What is Pr[M='aa' | C='bb']? Express your answer to 4 decimal places.

   (b) Suppose a message space is of 5-bit strings. Consider the one-time pad over on this message space. Given Pr[M=00100] = 0.1 and Pr[M=11011] = 0.9. What is Pr[C=00000]? Calculate answer to 5 decimal places with a leading 0.

6. What do you understand by perfect indistinguishability. Suppose you have designed an private key encryption encryption scheme which is perfectly secret. Does this imply that your scheme is perfectly indistinguishable. Justify your answer with complete proof. Consider a private key encryption scheme which is perfectly indistinguishable, and the receiver don't have the decryption key. Will he be able to generate the original message from received cipher-text or not? justify your answer.

7. (a) What do you understand by the *negligible function*? Give it's definition. Give two examples of negligible function and justify.

   (b) Which of the following is/are negligible function(s)? Justify.

   i. $\frac{1}{2^n}$

   ii. $\frac{1}{(\log n)!}$

   iii. $\frac{1}{(\log \log n)!}$

   iv. $\frac{1}{10^{10}}$

   v. $n^{\frac{1}{n}}$

   vi. $\frac{1}{2}$

   vii. $\frac{n}{2^n}$

   viii. $\frac{1}{n}$

   (c) Let f, g be *negligible functions*. Decide whether:

   i. $H(n) = f(n) + g(n)$

   ii. $H(n) = f(n) \times g(n)$

   iii. $H(n) = f(n)/g(n)$

   are necessarily *negligible functions* (for arbitrary f, g) or not. If it is, prove it. If not, give a counterexample.

8. (a) Give a formal definition of the Pseudo random generator. What Do you understand by expansion factor of a Pseudo random generator?

   (b) Say G is a pseudo random generator taking n-bit inputs and producing 2n-bit outputs. Which of the following are necessarily true? (The symbol '|' is used here for string concatenation.) Justify your answer.

   i. G(r) is computationally indistinguishable from a uniform, 2n-bit string if r is a uniform n-bit string.

   ii. G(0 | r) is computationally indistinguishable from a uniform, 2n-bit string if r is a uniform (n-1)-bit string.

   iii. r | G(r) is computationally indistinguishable from a uniform, 3n-bit string if r is a uniform n-bit string.

   iv. G(r) | G(r+1) is computationally indistinguishable from a uniform, 4n-bit string if r is a uniform n-bit string.

   v. G is one-way function.

9. What do you understand by one-way function? Let f, g be length preserving one-way function (so, e.g., $|f(x)| = |x|$). For each of the following functions h, decide whether it is necessarily a one-way function (for arbitrary f, g) or not. If it is, prove it. If not, show a counterexample.

   (a) $h(x) \stackrel{def}{=} f(x) \oplus g(x)$.

   (b) $h(x) \stackrel{def}{=} f(f(x))$.

   (c) $h(x_1 \parallel x_2) \stackrel{def}{=} f(x_1) \parallel g(x_2)$, ($\parallel$ means concatenation)

   (d) $h(x_1, x_2) = (f(x_1), x_2)$ where $|x_1| = |x_2|$.

10. Consider the below Private key encryption scheme: Let G be a pseudorandom generator with expansion factor l. The private key encryption is defined as follow:
Gen: on input 1^n, choose k= $\{0,1\}^n$ uniformaly at random and output it as a key.
Enc: input k and m $\epsilon\{0,1\}^j$, output cipher-text as $c := G(k) \oplus m$.
Dec: input k and c $\epsilon\{0,1\}^j$, output cipher-text as $m := G(k) \oplus c$.
Where j = l(n).
Prove or refute:

    (a) The private key encryption scheme defined above has the indistinguishable encryptions in the presence of an passive adversary (eavesdropper).

    (b) The private key encryption scheme define above has indistinguishable multiple encryptions in the presence of an eavesdropper.

11. Let $G : \{0,1\}^* \to \{0,1\}^*$ be a function that doubles the length of its input, i.e. $|G(s)| = 2 \cdot |s|$. Show an algorithm A (that does not necessarily run in polynomial time) for which

$$|\mathtt{Pr}[A(G(s)) = 1] - \mathtt{Pr}[A(r) = 1]| \geq 1/2$$

for n large enough. Can we conclude that "perfect PRGs" do not exist, why ?

12. Define the following function G taking n-bit inputs and producing (n+1)-bit outputs: G(x)=x||0, where || denotes concatenation. Which of the following attackers shows that this G is not a pseudorandom function? (Note: Only one of the below is true.)

    (a) On input an (n+1)-bit string y, output 0 if the first bit of y is 0.

    (b) On input an (n+1)-bit string y, output 1 if the first bit of y is 0.

    (c) On input an (n+1)-bit string y, output 0 if the last bit of y is 0.

    (d) On input an (n+1)-bit string y, output 0 if the first bit of y is equal to the last bit of y.

13. Let F be a pseudorandom function with 128-bit key and 256-bit block length. Which are the following functions G are pseudorandom generators?

    (a) G(x)=$F_x(0...0)||F_x(0...0)$, where x is a 128-bit input.

    (b) G(x)=$F_{0...0}(x)F_{1...1}(x)$, where x is a 256-bit input

    (c) G(x)=$F_x(0...0)$, where x is a 128-bit input.

    (d) G(x)=$F_x(0...0)||F_x(1...1)$, where x is a 128-bit input.

14. Given an efficiently-computable function $G : \{0,1\}^* \to \{0,1\}^*$ with $|G(x)| = l(|x|)$ consider the following experiment defined for an algorithm A and parameter n:

    (a) Choose random $s \in \{0,1\}^n$ and set $y_0 = G(s)$. Choose random $y_1 = \{0,1\}^{l(n)}$.

    (b) Choose a random bit $b \in \{0,1\}$.

    (c) Give y_b to A, who outputs a bit b'.

    say G is an *indistinguishable* PRG if for all probabilistic, polynomial-time algorithms A, there exists a negligible function ϵ such that

    $$\mathtt{Pr}[b' = b] \leq \tfrac{1}{2} + \epsilon(n)$$

    in the experiment above.

    Prove that this definition is equivalent to the definition of a pseudorandom generator.

15. state true or false with brief explanation:

(a) Any private-key encryption scheme that is CPA-secure must also be computationally indistinguishable.

(b) Any private-key encryption scheme that is CCA-secure must also be perfectly secret.

(c) Any private-key encryption scheme that is CCA-secure must also be CPA-secure.

16. Let F be a block cipher with 128-bit block length. Consider the following encryption scheme for 256-bit messages: to encrypt message $M = m_1 \| m_2$ using key k (where $|m_1| = |m_2| = 128$), choose random 128-bit r and compute the ciphertext r $\| F_k(\mathrm{r}) \oplus m_1 \| F_k(m_1) \oplus m_2$. Which of the following strategies would lead to a valid chosen-plaintext attack? (Note: only one is true.)

    (a) Choose random r and let m be arbitrary but not equal to r. Output messages $M_0 = r \| m$ and $M_1 = m \| m$. Output 0 if the second block of the challenge cipher text is all-0s.

    (b) There is no attack; this scheme is randomized, so it is CPA-secure.

    (c) Let m_1 and m_2 be arbitrary but distinct. Using the encryption, obtain an encryption $r \| c1 \| c2$ of $m2 \| m2$. Output messages $M_0 = m_1 \| m_1$ and $M_1 = m_1 \| m_2$. Output 0 if the third block of the challenge ciphertext is c_2.

    (d) Let m_1 and m_2 be arbitrary but distinct. Using the encryption , obtain an encryption $r \| c_1 \| c_2$ of $m_1 \| m_2$. Output messages $M_0 = m_1 \| m_2$ and $M_1 = m_2 m_1$. Output 0 if the third block of the challenge Ciphertext is c_2.

17. What do you understand by these terms: one way permutation, Pseudorandom generator, one way function, pseudorandom function, invertible pseudorandom generator. Give complete details (and if possible present an example illustrating the methods you describe) of how to use an X to design a Y where:

    (a) X = One-way permutation, Y = Pseudorandom generator.

    (b) X = Pseudorandom generator, Y = One-way function.

    (c) X = Pseudorandom generator, Y = Pseudorandom function.

    (d) X = Pseudorandom function, Y = Invertible pseudorandom function.

18. Let F be a block cipher with n-bit block length. Consider the following encryption scheme: to encrypt a message viewed as a sequence of n-bit blocks $m_1, m_2, , m_t$ using a key k, choose a random n-bit value r and then output the ciphertext r,$F_k(r+1+m_1), F_k(r+2+m_2), , F_k(r+t+m_t)$, where addition is done modulo 2n. Which of the following attackers demonstrates that this scheme is not computationally indistinguishable: (Note: Only one is true.)

(a) Let m be an arbitrary n-bit block, and output M_0=m,m and M_1=m,m1. Given challenge ciphertext r,c_1, c_2, output 1 if and only if $c_1 = c_2$.

(b) Let m be an arbitrary n-bit block, and output M_0=m and M_1=m,m. Given a challenge ciphertext, output 0 if the challenge ciphertext contains 2 blocks, and output 1 otherwise.

(c) Choose random n-bit blocks m and m', and output M_0=m,m and M_1=m,m. Given challenge ciphertext r,c_1, c_2, output 1 if and only if $c_1 = c_2$.

(d) Choose random n-bit blocks m_1, m_2, m_3, m_4, and output $M_0 = m_1, m_2$ and $M_1 = m_3, m_4$. Given challenge ciphertext r, c_1, c_2, output 0 if r= 0....0, and output 1 otherwise.

19. (a) Why probabilistic encryption scheme is required ? When the private key encryption scheme has indistinguishable encryption under chosen- plaintext attack? Explain in Detail. If a private key encryption scheme has indistinguishable encryption under chosen- plaintext attack, does this imply that this private key encryption scheme has indistinguishable multiple encryption under chosen- plaintext attack?

(b) What do you understad by Pseudo random function? Give formal definition. Assume the pseudorandom function exists, create a CPA-Secure fixed length private key encryption schemes using the Pseudorandom function. Prove how it is CPA-secure. Make proper assumptions if needed.

20. (a) What do you understand by Message integrity? What do you understand by Message Authentication code? Explain the construction of Fixed length MAC and Variable length MAC in Brief.

(b) Prove that the basic CBC-MAC is not secure when we consider the messages of different length. can you perform modification in Basic CBC-MAC for variable length messages So that it will be secure? Explain in detail.

(c) Let F be a block cipher with n-bit block length. Consider the message authentication code for 2n-bit messages defined by $Mac_k(m_1, m_2) = F_k(m_1 m_2)$. Which of the following gives a valid attack on this scheme?

i. Obtain tag t on message m,m, and then output the tag 0...0 on the message 0...0,m.

ii. Obtain tag t on message $m_1, m_2 (with m_1 ! = m_2)$, and then output the tag t on the message m_2, m_1.

iii. Obtain tag t on message m,0...0 (with ! = 0...0), and then output the tag t on the message 0...0,0...0.

iv. Obtain tag t on message m,0...,0, and then output the tag $t \oplus (1...1)$ on the message m,1...1.

21. (a) What do you understand by Hash function? What properties a Hash function should possess from Cryptographic point of view? Explain the Birthday Attack in brief. Explain these terms: *Encrypt and Authenticate*, *Authenticate then Encrypt*, *Encrypt then Authenticate.*

(b) Assume we want to use a hash function with output length as small as possible, subject to being collision resistant against a birthday attack running in time 2^192. Which hash function would be the best choice from these functions? SHA-3 with 384-bit output, SHA-1, MD5, SHA-2 with output truncated to 192 bits.

(c) Let H,H' be collision-resistant hash functions. Which of the following functions H"is NOT necessarily collision-resistant?

i. $H''(x) = H(x)H'(x)$, where $\|$ denotes concatenation.

ii. $H''(x) = H(x) \oplus H'(x)$.

iii. $H''(x) = H(H'(x))$.

iv. $H''(x) = H(x)\|0...0$, where $\|$ denotes concatenation.

1. (a) Explain Strong One way function and Weak One way function.
   (b) Prove "Weak one way functions exist if and only if strong one way functions exist".
   (c) Prove "A collection of one way functions exists if and only if one way functions exist".

2. Define the length-preserving, keyed function F by $F_k(x) = k \oplus x$. Prove that F is not a pseudo random function by describing and analyzing a concrete distinguisher.

3. Given a PRF F: $\{0,1\}^k x \{0,1\}^n \mapsto \{0,1\}^n$, construct a PRF G: $\{0,1\}^k x \{0,1\}^n \mapsto \{0,1\}^{2n}$, which is a secure PRF as long as F is secure.

4. Which of the following is collision resistant. Justify Your Answer

   (a) H'(m)=H(m)$\oplus$H(m)
   (b) H'(m)=H(H(H(m)))
   (c) H'(m)=H(m)[0,...,31] (i.e. output the first 32 bits of the hash)
   (d) H'(m)=H($|m|$) (i.e. hash the length of m)
   (e) H'(m)=H(m)$\oplus$H(m$\oplus 1^{|m|}$) (where m $\oplus 1^{|m|}$ is the complement of m)
   (f) H'(m)=H(m)$\|$H(m)
   (g) H'(m)=H(H(m))

   Assuming H: $M \mapsto T$ be a collision resistant hash function. and $\|$ represents the Concatenation

5. (a) What do you understand by Merkle-Demgard Transform? Explain its Construction Briefly.

   (b) Is it necessary that the Hash Function generated from Merkle-Demgard tranform will be Collision free if the initial Fixed length hash function was collision free? Prove your Answer.

6. Tell whether these are true or False and Justify your answer in brief (Either By explanation or by example):

   (a) Collision resistance implies 2nd-preimage resistance of hash functions.

   (b) collision resistance does not guarantee preimage resistance.

   (c) Let h_k be a keyed hash function which is a MAC algorithm (thus has the property of computation-resistance). Then h_k is, against chosen-text attack by an adversary without knowledge of the key k,

   i. both 2nd-preimage resistant and collision resistant; and

   ii. preimage resistant (with respect to the hash-input).

   (d) If either h_1 or h_2 is a collision resistant hash function, then $h(x) = h_1(x) \parallel h_2(x)$ is a collision resistant hash function.

7. *Note:* Read the Concept below before attempting the questions:
A Hash Family is Considered as a four Tuples (X,Y,K,H), where X a set (finite or Infinite) of Possible Messages , Y is the finite set of possible Message digests, K is the Key Space which is a finite set of possible Keys, for each k ϵ K, there exists a Hash Function $h_k \epsilon H$. A Pair (x,y) is valid pair if h_k(x)=y. Let $F^{X,Y}$ denotes the set of all hash functions. Suppose $|X| = N$, and $|Y| = M$. Then clearly, $\left|F^{X,Y}\right| = M^N$. Any hash Family F$\subseteq F^{X,Y}$ is known as (N,M) hash Family.
The Random Oracle Model Attempts to capture the concept of a ideal hash function. If a hash function h is well designed , it should be the case that the only efficient way to determine the value of h(x) for a given x is to evaluate the value x on the function x. This should not be the case that if $h(x_1), h(x_2)$ is already computed then there exists a x_3 such that $h(x_3)$ can be calculated from the previously computed hash values.
Theorem 1: suppose h $\epsilon F^{x,y}$ are chosen randomly and let $X_0 \subseteq X$. Suppose that the value h(x) have been determined (by querying for h) if and only if $x \epsilon X_0$. Then the Pr[h(x)=y] = 1/M for all $x \epsilon X - X_0$ and all yϵY.

From security Point of View, Some algorithms are discussed as below along wit there pseudo code:

Problem 1: PriImage
Instances: A hash Function h: $X \mapsto Y$
Find: x ϵ X such that h(x) = y.
Algorithms 1: Find-PreImage (h,y,Q)
choose any $X_0 \subset X, |X_0| = Q$

```
for each x in X_0:
    if (h(x)==y):
        return (x)
return (failure)
```

Problem 2: Second PreImage
Instances: A Hash function h: $X \mapsto Y$ and an element $x \epsilon X$.
Find: $x' \epsilon X$ such that x' != x and h(x')=h(x).
Algorithms 2: Find-Second-PreImage (h,x,Q)
y = h(x)
choose any $X_0 \subset X \{X_0, |X_0| = Q - 1$

```
for each x0 in  X_0$:
    if (h(x0)==y):
        return (x0)
return (failure)
```

Problem 3: Collision
Instances: A Hash function h: $X \mapsto Y$.
Find: $x, x' \epsilon X$ such that x' != x and h(x')=h(x).
Algorithm 3: Find-Collision (h,Q)
choose any $X_0 \subset X, |X_0| = Q$

```
for each x in X_0$:
      y_x = h(x)
if (y_x==y_x') for some x'!=x:
         return (x,x')
else return (failure)
```

Prove or refute:

(a) suppose that the hash function h: $Z_n x Z_n \mapsto Z_n$ is a linear function given by h(x,y)=ax+by mod n for a,b ϵZ_n and $n >= 2$ is a positive Integer. h follows the radical oracle model.

(b) For any $X_0 \subseteq X$ with $abs(X_0) = Q$, The Average case success probability of the algorithm 1 is p = 1-$(1 - 1/M)^Q$.

(c) For any $X_0 \subseteq X - \{x\}$ with $abs(X_0) = Q - 1$, The Average case success probability of the algorithm 2 is p = 1-$(1 - 1/M)^{Q-1}$.

(d) For any $X_0 \subseteq X$ with $abs(X_0) = Q$, The Average case success probability of the algorithm 3 is p = 1-[{(M-1)/M}*{(M-1)/M}*....{(M-Q+1)/M}]

8. if we define a hash function (or comparison function) h that will hash an n-bit binary string to an m-bit binary string, we can view h as a function from Z_{2^n} to Z_{2^m},it is tempting to define h using operation modulo 2^m. suppose that $n = m > 1$, and h:$Z_{2^m} \mapsto Z_{2^m}$ is defined as: h(x) $= x^2 + ax + b \bmod 2^m$. Prove that it is easy to solve second primage for any x ϵZ_{2^m} without having to solve the quadratic equation.

9. Consider a hash function h which is second PreImage and Collision resistant and Defined as $h : \{0,1\}^* \mapsto \{0,1\}^n$. Consider Another hash function h_1 which is defined as follow: $h_1 : \{0,1\}^* \mapsto \{0,1\}^{n+1}$ and given by rule :

$$h_1 = \begin{cases} 0 \| x & \text{if } x \epsilon \{0,1\}^n \\ 1 \| h(x) & \text{otherwise} \end{cases}$$ Prove that h_1 is not preimage resistant but still second preimage and collision resistant.

10. suppose h_1: $\{0,1\}^{2m} \mapsto \{0,1\}^m$ is a collision resistent function.

(a) Define h_2: $\{0,1\}^{4m} \mapsto \{0,1\}^m$ as follow:

i. write $x \epsilon \{0,1\}^{4m}$ as $x = x_1 \parallel x_2$ where $x_1, x_2 \epsilon \{0,1\}^{2m}$.

ii. Define $h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$.

Prove that h_2 is collision resistant.

(b) for any integer $i >= 2$, Define has function h_i: $\{0,1\}^{2^i m} \mapsto \{0,1\}^m$ recursively from h_{i-1} as follow:

i. write $x \epsilon \{0,1\}^{2^i m}$ as $x = x_1 \parallel x_2$ where $x_1, x_2 \epsilon \{0,1\}^{2^{i-1} m}$.

ii. Define $h_i(x) = h_{i-1}(h_{i-1}(x_1) \| h_{i-1}(x_2))$.

Prove that h_i is collision resistant.

11. Let m be a message consisting of l AES blocks (say l=100). Alice encrypts m using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $l/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

1. Suppose there is only one public channel between Alice and Bob and it has been given that no "active" adversary (there may be passive adversaries) is "active" over this channel. Alice want to send a message securely to Bob at time t So that Bob can get the message content after time t + t_1 where t_1 can be significantly large. Assuming that the channel have no transmission delay, Can you give a simple protocol for a successful communication between Alice and bob using the concepts of Private and Public key cryptography. If the adversary were active, can you tell that an active adversary is available, provided some message disruption have been made?

2. Group Theory

   (a) What do you understand by order of a group? Suppose, G is a multiplicative group of order n and g ϵ G. Then Prove that order of g devides n.

   (b) What do you understand by cyclic group. Suppose p is a prime then prove that Z_p^* is a cyclic group where Z_p^* is the set $Z_p - \{0\}$.

   (c) Explain Isomorphism, Homomorphism and Direct Product in the context of group?

3. (a) Using Extended Euclid Algorithms, Compute the following.
   i. $17^{-1} \bmod 101$.
   ii. $357^{-1} \bmod 1234$.
   iii. $3125^{-1} \bmod 9987$.

   (b) Solve these relations.

   - $x \equiv 12 \bmod (25)$
     $x \equiv 9 \bmod (26)$
     $x \equiv 23 \bmod (27)$

   - $13x \equiv 4 \bmod (99)$
     $15x \equiv 56 \bmod (101)$

4. Primality Testing

(a) Explain Solovay Strassen Primality Test Algorithm.

(b) Explain Miller-Robin Primality Test Algorithm. How it is different from the Solovay Strassen Primality test Algorithm?

(c) Assume that you have a computer performing 1 million bit operations per second. You want to spend only 2 hours on primality testing. What is larger number you can test using the following primality testing methods?

i. Trivial division method
ii. AKS algorithm
iii. Miller-Robin test

5. RSA

   (a) Suppose n= 84773093. The adversary somehow has learned the value of $\phi(n) =$ 84754668. Explain How can he learn the two factors p and q ? Here, Is there any need to learn the values of p and q if adversary only want to decrypt the message encrypted by and arbitrary e (co- prime to $\phi(n)$) and n?

   (b) Consider the RSA cryptosystem and an encryption exponent e =3. show that plaintext message m can be recovered if it is enciphered (encrypted) and sent to three different entities having the pairwise relatively prime moduli n_1, n_2, n_3.

6. Users A and B use the Diffie-Hellman key exchange techniques with a common prime q = 71 and a primitive root $\alpha = 7$.

   (a) If the user A has private key $X_A = 69$, what is the As public key Y_A ?

   (b) If the user B has private key $X_B = 15$, what is the Bs public key Y_B ?

   (c) What is the shared secret key between A and B?

7. It is well known that there is an active attack on the Diffie-Hellman Key exchange Techniques which is known as the "Man in the Middle attack"? Explain this attack in detail. The station to station key agreement method on the Diffie-Hellman uses authentication to thwart this serious attack. Explain this method.

8. Let G be a finite cyclic group (e.g. G=Z_p) with generator g. Suppose the Diffie-Hellman function $DH_g(g^x, g^y) = g^{\{xy\}}$ is difficult to compute in G. Which of the following functions is also difficult to compute: As usual, identify the f below for which the contra-positive holds: if f(,) is easy to compute then so is $DH_g(,)$. If you can show that then it will follow that if DH_g is hard to compute in G then so must be f.

   (a) $f(g^x, g^y)=(g^2)^{\{x+y\}}$

   (b) $f(g^x, g^y)=g^{\{xy\}^{0.5}}$

   (c) $f(g^x, g^y)=(g^{0.5})^{\{x+y\}}$

   (d) $f(g^x, g^y)=g^{\{xy+x+y+1\}}$

9. (a) Explain The ElGamal scheme in detail. Consider an ElGamal scheme with a common prime number q = 71 and a primitive root $\alpha = 7$. If the recipient B has the public key $Y_B = 3$ and the sender A chooses the random integer $X_A = 2$, what is the ciphertext of the plaintext message M = 30?

   (b) What is the discrete logrithm of a prime number p.Define formally the elliptic curve discrete logrithm problem (ECDLP) with the adversary A's advantage.

10. Let two parties A and B agree on the following digital signature scheme. Entity A signs a binary message m of arbitrary length. Entity B can verify this signature by using the public key of A.
Entity A perform the following step for key generation:

(a) select two prime p and q such that q | (p-1).

(b) select random integer g with 1< g <p-1, such that $\alpha = g^{\{(p-1)/q\}} \pmod p$ and $\alpha > 1$.

(c) Select a private key a (integer), $0 < a < q$.

(d) Compute $y = \alpha^a \pmod p$.

Public key of A is (p, q, α, y).
After key generation, A generates a signature on m as follows:

(a) Select a random secret integer k, $1 < k < q$.

(b) Compute $r = \alpha^k \bmod p$, $e = H(m\|r)$, and $s = (ae + k) \bmod q$.

(c) Select two random secret integers u and v, $0 < u < q$ and $0 < v < q$, and compute $r' = r\alpha^{-u}y^v \bmod p$.

(d) Compute e' = H(m||r') such that e'= e-v and s'= s-u. A then sends the signed message (m,(e',s')) to the verifier B. Here H is a hash function.

Devise a verification algorithm for the party B.Prove the verification equation mathematically.

2. State and prove the Fermat's little theorem. Use it to show that `msb` is a hard-core predicate for the discrete-logarithm function. Illustrate in detail, how would you design a provably secure pseuro-random generator whose security is founded on the hardness of computing the discrete-logarithm.

3. Answer the following on cryptanalysis (i.e. breaking of cryptosystems).

(a) Consider the following private-key encryption scheme: The shared key is $k \in \{0,1\}^n$. To encrypt message $m \in \{0,1\}^n$, choose random $r \in \{0,1\}^n$ and output $(r, F_r(k) \oplus m)$, where F is a block cipher. Show that this scheme is not CPA-secure.

(b) Let q_j denote the j^{th} prime number, that is $q_1 = 2, q_2 = 3$, and so on. Let

$$p(k) = \left(1 + \prod_{j=1}^{k} q_j\right)$$

For some k if $p(k)$ turns out to be prime, then show that discrete-logarithm is *easy* to compute in the cyclic group $\mathbb{Z}^*_{p(k)}$.

(c) Show that the basic CBC-MAC as described in class is insecure if the sender authenticates messages of different lengths.

4. A set X is said to closed under a binary operation $\circ$ if for all $a \in X$, $b \in X$, it is true that $a \circ b \in X$. For example, the set of integers are closed under addition, subtraction, and multiplication but not division. Answer the following questions on the set $\mathbb{S}$ of all negligible functions:

   (a) Show that $\mathbb{S}$ is closed under addition but not closed under subtraction (the inverse operation of addition).

   (b) Show that $\mathbb{S}$ is closed under multiplication but not closed under division (the inverse operation of multiplication).

   (c) Can you think of a non-trivial binary operation $\circ$ such that $\mathbb{S}$ is closed under both $\circ$ as well as its inverse operation? Justify your answer.

   (d) Can you think of a non-trivial binary operation $\square$ such that $\mathbb{S}$ is *not* closed under both $\square$ as well as its inverse operation? Justify your answer.

   (e) Define a relation on $\mathbb{S}$ as follows: aRb iff $(a-b) \notin \mathbb{S}$. Is R an equivalence relation? Prove your answer.

5. This question is on perfect secrecy and historical ciphers:

   (a) An encryption scheme is formally defined by algorithms `Gen`, `Enc` and `Dec` as well as a message space $\mathcal{M}$. Give formal specifications of these components for the shift cipher, the mono-alphabetic substitution cipher, and the Vigenere cipher (for the latter, you may assume the key-phrase always has length ℓ).

   (b) Prove or refute: Every encryption scheme for which the size of the key-space is equal to the size of the message-space, and for which the key is chosen uniformly at random from the key-space, is perfectly secret.

   (c) Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.

   (d) What is the largest plaintext space $\mathcal{M}$ you can find for which the mono-alphabetic substitution cipher provides perfect secrecy? (Note: $\mathcal{M}$ need not contain only valid English words.)

   (e) Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$ every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$

$$\Pr[M = m | C = c] = \Pr[M = m' | C = c]$$

1. Assume that the function $F_k : \{0,1\}^2 \to \{0,1\}^2$ where $F_k(x) = [(x^{k \bmod x} + k^{x \bmod k}) \bmod 4]$, $k \in \{0,1\}^2$, is pseudorandom (it really isn't for the key space is too small but it does ease the calculations). Answer the following:

   (a) Write the entire truth table for F_k where k is 3 (that is k is the bit sequence 11). Is F_k a bijection/permutation?

   (b) Using F_k as a PRF, what is the tag generated by CBCMAC (made secure by prepending length) on the message $m = 1101$ for $k = 3$?

   (c) Using CBCMAC created above and F_k as a PRF in the randomized-counter mode of operation to obtain a CPA-secure encryption scheme, construct a CCA-secure encryption scheme using the `encrypt-then-authenticate` paradigm. What is the encryption of $m = 110110$ if $r = 01$, with $k = 3$.

2. Consider a completely connected network $\mathcal{N}$ of four nodes $\{A, B, C, D\}$. The node A wishes to establish a secret key with node D using the Diffie-Hellman key exchange algorithm, given a prime p and a generator g of $\mathbb{Z}_p^*$. However, *one* of the (six) channels in the network is suspected to be actively corrupt by a computationally *unbounded* adversary who can easily solve the discrete logarithm problem as well as modify the messages sent across the channel. The other five channels are (simultaneously) eavesdropped by another independent computationally bounded adversary. Design a protocol for key agreement between A and D that works correctly and securely no matter which channel is actively corrupt.

3. Assuming $H : M \to T$ to be a collision resistant hash function, which of the following is collision resistant; *prove* your answers.

   (a) $H'(m) = H(m) \oplus H(M \oplus 1^{|m|})$

   (b) $H'(m) = H(m||m)$

   (c) $H'(m) = H(m[0, ..., |m| - 2])$ *i.e.* Hash without last bit

   (d) $H'(m) = H(m)||H(m)$

   (e) $H'(m) = H(H(H(m)))$

4. For each of the following modifications to the Merkle-Damgard transform, *prove* whether the result is collision resistant or not (notations used are from assignment).

   (a) Modify the construction so that instead of outputting $z = h^s(z_B||L))$, the algorithm outputs $z = (z_B||L)$.

   (b) Instead of using a fixed IV , choose $IV \leftarrow \{0,1\}^n$ and define $z_0 = IV$. Then, set the output to be $z = (IV, h^s(z_B||L))$.

   (c) Instead of using a fixed IV , just start the computation from x_1. That is, define $z_1 = x_1$ and compute $z_i = h^s(z_{i-1}||x_i)$ for $i = 2, ..., B$.

5. Suppose $N = 84773093$ in RSA algorithm. The adversary somehow has learned the value of $\phi(N) = 84754668$ Explain how the adversay can learn the two factors p and q of N? Here, is there any need to learn the values of p and q if adversary only wishes to decrypt the message encrypted by an arbitrary e (co-prime to $\phi(N)$)?

6. Explain the El-Gamal public-key scheme in detail. Prove that is it CPA-secure.

7. If $2^n + 1$ is an odd prime for some integer n, prove that n is a power of 2.

QUESTION 1

Describe how to establish a secret-key between Alice and Bob (in the presence of an eavesdropper) in each of the following cases:

a. The eavesdropper is computationally bounded and the decisional Diffie-Hellman assumption is true.

b. There is a partial-secure channel connecting Alice and Bob wherein the computationally unbounded eavesdropper can access up to any $t < n$ among the n blocks (of fixed size) transmitted.

c. The eavesdropper is computationally unbounded but there is a quantum channel connecting Alice and Bob.

d. The eavesdropper is computationally unbounded but there is a noisy channel (that corrupts up to any 2 bits of every 4 bits sent) connecting Alice and Bob.

QUESTION 2

In Shamir's (t,n)-secret sharing scheme, the size of each share is same as the size of the secret. This is inefficient to share large secrets (storage required is n times the original secret). Assuming that the adversary is computationally bounded and using the techniques of modern cryptography answer the following:

a. Design a new *computationally secure* (t,n)-secret sharing scheme such that the total size of all the shares is nearly the size of the secret.

b. Using your idea along with Shamir's, design a new hybrid (s,t,n)-secret sharing scheme such that the secret remains perfectly secure for any collusion of up to s shares, and is computationally secure for any collusion up to t shares. What is the size of each share in your hybrid design? (Note that at $s = t$ it is like Shamir's secret sharing and at $s = 0$ it is like your computational secret sharing scheme).

QUESTION 3

An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out five at a time, there were two eggs left. The same happened when she picked them out nine at a time, but when she took them seven at a time they came out three. What is the smallest number of eggs she could have had? What is the second-smallest number of eggs she could have had? In general, what is the k^{th}-smallest number of eggs she could have had? Prove your answers.

QUESTION 4

Answer the following with respect to the Byzantine agreement problem.

a. Prove that there exists *no* protocol for Byzantine agreement among three nodes, one of which is actively corrupted by a computationally unbounded adversary.

b. Design a Byzantine agreement protocol among three nodes of which one of them can be actively corrupted by a computationally *bounded* adversary, assuming that digital signatures exist. Prove the correctness of your protocol.

QUESTION 5

Alice and Bob are very shy but would nevertheless like to find out whether they are interested in each other. Both Alice and Bob have their secret bits x and y that encodes whether they are interested in the other person; $x = 1$ means that Alice is interested in Bob, $x = 0$ means that Alice is not interested, and so on for y. Design and analyze a protocol that will help Alice and Bob to *securely* find out whether or not they are interested in each other, assuming that the DDH assumption is true.

QUESTION 7

Let q_j denote the j^{th} prime number, that is $q_1 = 2, q_2 = 3$, and so on, and $\alpha_j \geq 0$ is some integer. Let

$$p(k) = \left(1 + \prod_{j=1}^{k} q_j^{\alpha_j}\right)$$

Show (by exhibiting a polynomial-time attack) that the Diffie-Hellman key establishment protocol in the cyclic group $\mathbb{Z}^*_{p(k)}$ is *not* secure, for any k where $p(k)$ is a prime.

Book - Introduction to modern Cryptography (The exact edition of the book will be posted on Moodle)

Problems -
5.1, 5.4, 5.5, 5.8, 5.9, 5.15,

7.4, 7.6, 7.8, 7.11, 7.14, 7.21, 7.22,

9.2, 9.3,

10.1, 10.4, 10.9, 10.11, 10.13, 10.14,

12.1, 12.4, 12.5, 12.6, 12.8, 12.9