Practice Problems
Cryptography and Network Security

1. Lecture 1: Introduction

   (a) Alice and Bob wish to resolve a dispute over telephone. We can encode the possibilities of the dispute by a binary value. For this they engage a protocol:

      i. **Alice** $\rightarrow$ **Bob**: Alice picks up randomly an x, which is a 200 bit number and computes the function $f(x)$. Alice sends $f(x)$ to Bob.
      ii. **Bob** $\rightarrow$ **Alice**: Bob tells Alice whether x was even or odd.
      iii. **Alice** $\rightarrow$ **Bob**: Alice then sends x to Bob, so that Bob can verify whether his guess was correct.

   If Bob's guess was right, Bob wins. Otherwise Alice has the dispute solved in her own way. They decide upon the following function, $f : X \rightarrow Y$, where X is a random variable denoting a 200 bit sequence and Y is a random variable denoting a 100 bit sequence.

   The function f is defined as follows:

   $$f(x) = (\text{ the most significant 100 bits of } x) \vee (\text{the least significant 100 bits of } x), \quad \forall x \in X$$

   Here $\vee$ denotes bitwise OR.

   Answer the following questions in this regard:

      i. Design a suitable strategy for Bob to guess the parity of x.
      ii. If Alice is honest, what is the probability of Bob to be successful in guessing whether x is even or odd correctly?
      iii. What is Alice's probability of cheating Bob?
      iv. Give a brief reasoning as to whether you would suggest Alice and Bob to use the function f.

   (b) What happens when the Boolean function is replaced by bit-wise XOR? Rework the above sub-parts for this change, and explain which Boolean function would you prefer for the given application.

2. Lecture 2: Overview on Modern Cryptography

   (a) Cite examples from real life, where the following security objectives are needed:

      i. Confidentiality
      ii. Integrity
      iii. Non-repudiation

   Suggest suitable security mechanisms to achieve them.

   (b) Give a real life example where both confidentiality and integrity is needed. Explain why encryption alone does not provide integrity of information.

3. Lecture 3: Introduction to Number Theory

(a) A student has been asked to solve the following problem: Compute the seventh root of 23 in Z_{77}^* by using the Extended Euclidean Algorithm and the Square and multiply algorithm. Help him to get the solution by approaching the problem as follows:

i. Compute d, the inverse of 7 modulus $\phi(77)$, where $\phi(.)$ indicates the Euler's Totient function. Use the extended Euclidean algorithm for this.

ii. Compute 23^d modulus 77 using the square and multiply algorithm.

(b) A student has been asked to solve the following seemingly simple problem: $x \equiv 2^{1990} \text{mod } 1990$. Help her to get the solution by approaching the problem as follows:

i. Factorize 1990 into prime factors.

ii. For all the prime factors, p_i (or its power as may be the case), express the given congruence as $x \equiv a_i \text{mod } p_i$.
(**Hint:** Apply Fermat's little Theorem, if p is prime, for any positive integer a, $a^{p-1} \equiv 1 \text{mod } p$.)

iii. Apply Chinese Remainder Theorem (CRT) to get the solution of the original congruence.

4. Lecture 4: Probability and Information Theory

(a) Suppose that four digit Personal Index Numbers (PINs) are randomly distributed. How many people must be in a room such that the probability that two of them have the same PIN is at least $\frac{1}{2}$?

(b) A very important cryptographic question is to check whether a list contains a collision or not. The trivial idea is to consider all pairs of the elements of the list with n elements. Thus this search requires $n(n-1)/2$ tests. However the search for collisions can be performed more efficiently in $O(nlogn)$ operations using the following techniques:

i. Sort the list by an efficient sorting algorithm and comparing each element with its immediate successor. Examine if any collision can be missed in such a method and modify the algorithm accordingly.

ii. Apply the following hash function, $h(x) =$ last b bits of x. For any new element x, look into the hash table, T at the address $h(x)$. If the location is unoccupied, indicated by an empty string τ, then the element is stored. Else it is checked whether $T[h(x)] = x$, in which case a collision is reported, else there is no collision. Examine the above algorithm to see that a collision can be missed if there is a three-way collision, ie. $\exists x, y, z$, such that $y = z, x \neq y$ and $h(x) = h(y) = h(z)$. Show that $b \approx 2n/3$, ensures that the probability of such a three way collision is reduced significantly.

(c) From Information Theoretic point of view answer the following questions:

i. How many $0-1$ questions are needed to ascertain a number within 0 and 63?

ii. You are given 12 balls, all equal in weight except for one that is either heavier or lighter. You are also given a two-pan balance to use. In each use of the balance you may put any number of the 12 balls on the left pan, and the same number on the right pan, and push a button to initialize the weighing. There are three possible outcomes, either the weights are equal or the balls on the left are heavier or lighter. What is the minimum number of weighings needed to determine which is the odd ball and whether it is heavier or lighter than the others.

5. Lectures 5 and 6: Classical Cryptography and Cryptanalysis

(a) Which of the following digrams (figure 1) represent *injective functions*?

(b) Consider a sequence $a_1, a_2, a_3 \ldots$, such that a_n is the residue of p^{n+2} modulo 24. Prove that for any prime p, this sequence is periodic with period 2.

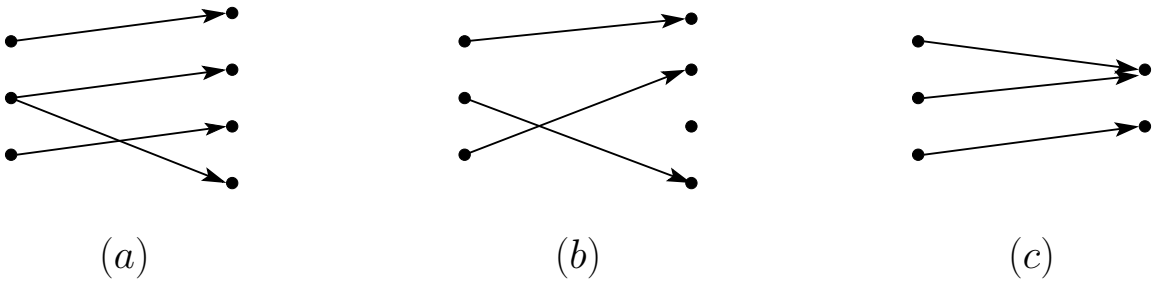

Figure 1: Digrams for Question 1

(c) The following cryptogram has been received:

`ECGUCTUJKHV`

The encryption algorithm is as follows. Let x_1, x_2 be the roots of the polynomial $x^2 + 3x + 1$. Each letter of the plaintext is replaced with its position in the English alphabet (A is 1 and Z is 26). Then to every number the value of the polynomial $f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$ either at x_1 or at x_2 is added. After that the numbers obtained are replaced with letters. Recover the plaintext. (**Moral of the story:** Repeating complex steps may lead to a very trivial cipher.)

(d) Let l be a positive integer. Let γ be the set of all Vignere ciphers of key length l. Denoting $\circ$ the composition of two functions, prove that $(\gamma, \circ)$ is a *group*.

What is the product cipher of two Vignere ciphers with distinct key lengths?

(e) S_1 and S_2 are two Vignere ciphers with keys of length m_1 and m_2 respectively, with $m_1 > m_2$. Prove that if $m_1 \neq 0 \bmod m_2$, then $S_1 \times S_2 \neq S_3$, where S_3 is the Vignere cipher with keyword $lcm(m_1, m_2)$.

(f) Suppose E_1 and E_2 are two encryption methods. Let t_1 and t_2 be two keys belonging to Z_{26}. Define E_1 be an encryption, which involves multiplying the plaintext, m also belonging to Z_{26} by t_1. Similarly, define E_2 as an encryption which involves adding the input with t_2, modulo 26. Answer the following questions regarding the above ciphers and their composition:

i. What is the requirement of t_1 for the cipher E_1 to be an encryption algorithm? (Note encryption algorithms are reversible).

ii. What is the composition of the ciphers, denoted by $E_1 \circ E_2$ popularly known as in classical cryptography? Note given a plaintext, m from Z_{26}, the ciphertext c is given by $c = t_1 m + t_2 (\text{mod } 26)$.

iii. What is the brute force complexity to break the cipher (i,e what is the total number of values of t_1, t_2)?

iv. Develop a meet in the middle attack against the cipher, and show that there are exactly 38 encryptions required.

6. Lecture 7, 8 and 9: Shannon's Theory

(a) Suppose that a cryptosystem has two keys k_1 and k_2, three messages m_1, m_2, and m_3, and three ciphertexts c_1, c_2, and c_3. Assume that the probability function for the message variables are as follows:

$$\begin{array}{lllll} p_M(m_1) & = & p_M(m_2) & = & \frac{1}{4} \\ p_M(m_3) & = & \frac{1}{2} & & \end{array}$$

Suppose that the following table describes how the different keys act on the messages to produce ciphertexts: Assuming that all keys are equally likely compute the key equivo-

	m_1	m_2	m_3
k_1	c_2	c_1	c_3
k_2	c_3	c_3	c_2

	m_1	m_2	m_3
k_1	c_2	c_4	c_1
k_2	c_1	c_3	c_2
k_3	c_3	c_1	c_2

Table 1: An Encryption Function

cation of the cryptosystem.

(b) Consider a cipher that has three keys, three plaintexts, and four ciphertexts that are combined using the following encryption table (table 2):
Suppose further that the plaintexts and keys are used with the following probabilities:
$f(m_1) = f(m_2) = \frac{2}{5}$; $f(m_3) = \frac{1}{5}$
$f(k_1) = f(k_2) = f(k_3) = \frac{1}{3}$.
Does the above cryptosystem has perfect secrecy?

(c) Suppose that the key equivocation of a certain cryptosystem vanishes, i.e $H(K|C) = 0$. Prove that even a single ciphertext uniquely determines the key.

(d) Show that the unicity distance of the Hill Cipher over Z_{26} (with an $m \times m$ encryption matrix) is less than m/R_L, where R_L is the redundancy of the language.

(e) Suppose S_1 is the *Shift Cipher* (with equiprobable keys) and S_2 is the *Shift Cipher* where keys are chosen with respect to some probability distribution $P_{\mathcal{K}}$ (which may not be equiprobable). Prove that $S_1 \times S_2 = S_1$.

(f) Consider the problem of sorting n elements. Any generalized sorting algorithm takes these n numbers and peforms comparisons to sort the numbers. The complexity of the algorithm is measured by the number of comparisons required. Note that the trace of the comparisons help one to trace back from the sorted array to the initial array of numbers. That is the comparison traces have the same information as the initial unsorted array. Based on the above idea, conclude that the sorting of n elements cannot be done better than $O(nlogn)$ complexity.
Hint: One comparison provides at most one bit of information of the initial sorted array, since you know the relative ordering of two numbers in the unsorted array.

7. Lecture 10-16: Symmetric Key Ciphers, DES, AES and Cryptanalysis

(a) DES (Data Encryption Standard) although an elegantly designed cipher has become old. Its $n = 56$ bit key is being challenged by the present day computation power. As an alternative, it was thought of applying DES twice, i.e in creating a product cipher $DES' = DES \times DES$. If the key space of DES was $K = \{0,1\}^n$, the key size of the product cipher is expected to be $K_1 \times K_2 = (K_1, K_2)$, where $K_1, K_2 \in K$. The plaintext of the cipher is denoted by $P = \{0,1\}^m$ and the cipher is endomorphic (the plaintext and the ciphertext are the same set). In regard to this composed cipher answer the following questions:

i. What is the property in the DES construction which helps to increase the key length by performing such composition? (Another way of asking the question is: why is DES not idempotent?)

ii. Using the DES cipher an attacker obtains l pairs of plaintexts and ciphertexts: $(p_1, c_1), \ldots, (p_l, c_l)$. The key is say (K_1, K_2) but unknown to the attacker (obviously, else why will he/she be an attacker).

Prove that for all $1 \leq i \leq l$, $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i)\ \forall i$, where $1 \leq i \leq l$.

iii. Prove that of all the possible keys (K_1, K_2), the expected number of keys for which $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i)\ \forall i$, where $1 \leq i \leq l$, is about 2^{2n-lm}.

iv. Suppose $l \geq 2n/m$, what can you say to the attacker to help him in developing an attack against the composed cipher DES'?

v. The attacker starts building up two lists: L_1 and L_2. Each entry in the list L_1 and L_2 has l tuples of elements of P followed by an element from K. The lists are filled with all possible keys.
The lists are now sorted in a lexicographic manner on the l tuples. The attacker now does a linear search to find out the common l tuples in the lists.
Explain how does the attacker maintain the list and how does this approach help him to find out the correct key? Show that the amount of memory required by the attacker is $2^{n+1}(ml + n)$ bits and number of encryptions and/or decryptions required to identify the key is $l2^{n+1}$. (Hint: Use the distinguisher: for the correct key $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i)\ \forall i$)

vi. Into what class does the above kind of attack fall?

(b) Let $DES(x, K)$ represent the encryption of plaintext x with key K using the DES cryptosystem. Suppose $DES(x, K)$ and $y' = DES(c(x), c(K))$, where $c(.)$ denotes the bitwise complement of its argument. Prove that $y' = c(y)$.
That is if we complement the plaintext and the key in DES, then the ciphertext also gets complemented.
Note: This can be proved by the high level description of DES, the actual structure of S-Boxes or other component functions are irrelevant to this result.

(c) i. Consider an SPN (Substitution Permutation) cipher on input x, with number of rounds being indictated by N_r. Prove that if the last round has a permutation layer then it does not increase the strength of the cipher.

ii. Consider an invertible Substitution operating on m bits, where m is an integer. Prove that it is a permutation from $\{0,1\}^m$ to $\{0,1\}^m$.

(d) Suppose that X_1, X_2 and X_3 are independent discrete random variables defined on the set $\{0,1\}$. Let ϵ_i denote the bias of X_i, for $i = 1, 2, 3$. Prove that if $X_1 \oplus X_2$ is independent of $X_2 \oplus X_3$, then either $\epsilon_1, \epsilon_3 = 0$ or $\epsilon_2 = \pm 1/2$.

(e) For AES-128 answer the following questions:

i. In one sentence answer, why is Boomerang attack expected to be more powerful than a conventional Differential attack?

ii. Consider two keys of AES-128, which are related as: their differential value is $(\alpha, 0, 0, 0)$, where α is a given 32-bit value $\neq 0$. Determine the propagation of the 4-round differentials of the round keys through the key scheduling algorithm.

(f) Let y be the output of an SPN (Substitution Permutation Network) Cipher on input x, where π_S and π_P are the substitution and permutation transformation of the ciphers. Thus,

$$y = SPN(x, \pi_S, \pi_P, (K^1, \ldots, K^{N_r+1}))$$

where $(K^1, \ldots, K^{N_r+1})$ is the key schedule. Find a substitution π^*_S and π^*_P such that:

$$x = SPN(y, \pi^*_S, \pi^*_P, (K^1, \ldots, K^{N_r+1}))$$

(g) Suppose that $\pi_S : \{0,1\}^m \rightarrow \{0,1\}^n$ is an S-Box. Let the pair (a, b), where $a = (a_1, \ldots, a_m)$, $b = (b_1, \ldots, b_n)$, $a_i, b_j \in \{0,1\}$ and $1 \leq i \leq m; 1 \leq j \leq n$ denote the linear approximation, $(\bigoplus_{i=1}^{m} a_i x_i) \oplus (\bigoplus_{j=1}^{n} b_j y_j) = 0$
Let $N_L(a, b)$ be an entry in the Linear Approximation Table, that is the number of input and output pairs for the S-Box which satisfy a given approximation (a, b).
Prove the following facts about the function $N_L(a, b)$:

i. $N_L(0,0) = 2^m$

ii. $N_L(a,0) = 2^m - 1$ for all integers a such that $0 \leq a \leq 2^m - 1$

iii. For all integers a such that $0 \leq a \leq 2^m - 1$, it holds that:

$$\sum_{a=0}^{2^m-1} N_L(a,b) \quad = \quad 2^{2m-1} \pm 2^{m-1}$$

8. Lecture 17: Overview on S-box design Principle

   (a) Consider the Boolean fuctions $f(x) : \{0,1\}^m \rightarrow \{0,1\}$ and $g(y) : \{0,1\}^n \rightarrow \{0,1\}$. Assume f and g operates on statistically independent variables.
   Denote $W_f(w) = \sum^x (-1)^{f(x) \oplus x.w}$, where $w \in \{0,1\}^m$.
   Answer the following questions:

   i. Prove that if f is balanced $W_f(0) = 0$.

   ii. Prove that if f is a balanced function then $f(x) \oplus g(y)$ is always balanced.

   iii. If the non-linearity of f is denoted by N_f, then prove that $N_f = 2^{n-1} - \frac{1}{2}|W_{max}|$, where $|W_{max}|$ is the maximum absolute value among all the $W_f(w)$, $\forall w$.

   iv. A Boolean function f in n variables is called bent if and only if the values of $W_f(w)$, $\forall w$ are all $\pm 2^{n/2}$. Prove that the Boolean function $f(x) \oplus g(y)$ is bent if f and g are bent functions.

   v. Using the above results prove that the Boolean function $x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus \ldots \oplus x_{n-1}x_n$ is a bent Boolean function.

9. Lecture 18: Modes of Block Ciphers

   (a) Explain that the Electronic Code Book (ECB) mode is not a secured mode of encryption and highlight the problems with this mode.

   (b) A hardware designer intends to develop a hardware chip for an encryption mode, which supports pipelining. From the choices of Cipher Block Chaining, Cipher Feedback Block, and Output Feedback Block explain which are suitable candidates for such an application.

10. Lecture 19-22: Stream Ciphers and Pseudorandomness

    (a) We are using the m-sequence generator created according to the primitive polynomial $x^{10} + x^3 + 1$. A trial consists of initialization of the shift register with 10 bits, running the shift register with feedback according to the above connection polynomial for 500 steps, and the reading out the 500 bits of the LFSR.
    The following table shows some *Initial Register Setting* and *Register Contents after 500 Steps*.

Table 2: Some pairs of register settings displaced by 500 steps

Initial Register Setting		Register Contents after 500 Steps
0100111010		1001000001
0111010010		1101000111
1011010110		1100101000
1000101101		1011011011

Using the above values can you figure out if the shift register was initialized with 1011000101, what would be the register contents after 500 steps? Can you say how many minimum such input and output pairs are needed to obtain the output for all possible non-zero inputs (i.e all inputs for which all input bits are not zero).

(b) Reconstruct an LFSR of the shortest length which generates the sequence $\{1, 0, 0, 0, 1, 1, 1, 1\}$ by using Berlekamp-Massey Algorithm.

(c) The following is the description of the A5/1 key stream generator (refer **Fig 2**). It consists of three LFSRs denoted by R_1, R_2 and R_3, with respective lengths of 19, 22, and 23 bits. The total content of all the three LFSRs is thus $19 + 22 + 23 = 64$ bits. We refer the 64 bit initial contents of the three LFSRs as the key of the cipher. $R_i[n]$ is used to refer to the n^{th} bit of the register R_i, where $i = 1, 2, 3$, and n starts from 0. Each LFSR has one clocking tap: $R_1[8], R_2[10], R_3[10]$. At each clock cycle, one key stream is generated as follows:

- The three LFSRs make a clocking vote according to the majority of the current three clocking taps.
- Each R_i compares the voting result with its own clocking tap. If they are equal, R_i is shifted:
  - a feedback bit is computed by XORing the contents of a fixed subset of cells of R_i, i.e the feedback for R_1, R_2 and R_3 is: $R_1[18] \oplus R_1[17] \oplus R_1[16] \oplus R_1[13]$, $R_2[21] \oplus R_2[20]$, and $R_3[22] \oplus R_3[21] \oplus R_3[20] \oplus R_3[7]$ respectively.
  - the content of all cells in R_i (except the leftmost) are shifted to the left by one position simultaneously
  - $R_i[0]$ is updated by the precomputed feedback.
- Output the bit $R_1[18] \oplus R_2[21] \oplus R_3[22]$.

Answer the following questions regarding the above key stream generator:

i. Show that when R_1 is loaded with a special initial state, then its state remains the same in the future.

ii. Compute the number of 64 bit keys (number of initial states of the three LFSRs) so that the stream cipher generates 64 bit all zero key stream.

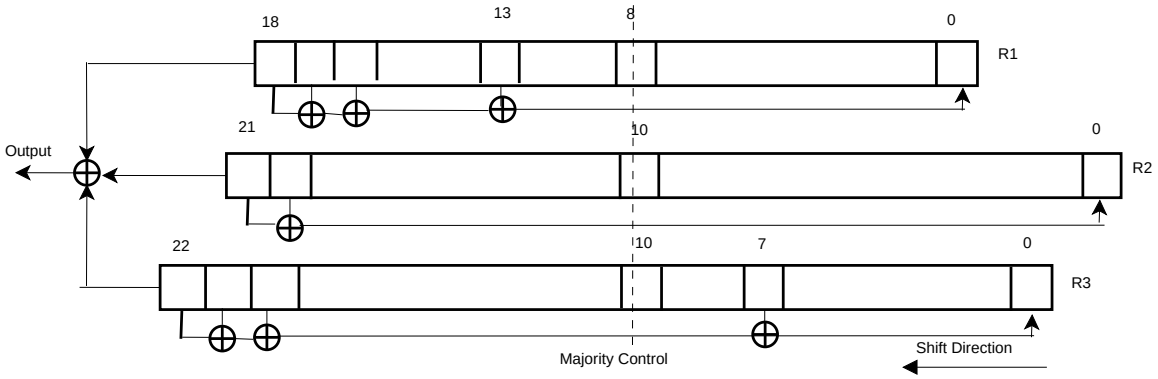

Figure 2: A5/1 Key Stream Generator

.

(d) Explain that neither one round nor two rounds of the Fiestel cipher (consider DES) is a pseudorandom generator.

(e) Design a finite state machine with n states (called as cells), st. each i^{th} cell in the t^{th} time instance propagates according to the following rules:

$$\begin{aligned} s_i^t &= s_i^{t-1} \oplus s_i^{t-1} \oplus s_i^{t-1} \text{ (for odd cells)} \\ s_i^t &= s_i^{t-1} \oplus s_i^{t-1} \text{ (for even cells)} \end{aligned}$$

The boundary cells are null, ie. $s_{-1} = s_n = 0$. Consider an n-stage machine and the sequence generated by the zeroth cell, ie. $s = s_0^t$, where t denotes the time instance. Examine the sequence generated and test it for pseudorandomness by performing the 5 basic statistical tests.

11. Lecture 23-26: Hash Functions and MACs

(a) Suppose that $f : \{0,1\}^m \rightarrow \{0,1\}^m$ is a preimage resistant bijection. Define $h : \{0,1\}^{2m} \rightarrow \{0,1\}^m$ as follows. Given $x \in \{0,1\}^{2m}$, write:

$$x \quad = \quad x'||x''$$

where $x', x'' \in \{0,1\}^{2m}$. Then define

$$h(x) \quad = \quad f(x' \oplus x'').$$

Prove that h is not second preimage resistant.

(b) A message authentication code can be produced by a block cipher in CFB mode. Given a sequence of plaintext blocks, $x_1, \ldots, x_n$, the IV is x_1. Then the sequence, $x_2, \ldots, x_n$ is encrypted using key K in CFB mode, obtaining the ciphertext sequence $y_1, \ldots, y_{n-1}$. Thus, $y_i = e_K(y_{i-1}) \oplus x_{i+1}$, where $1 \leq i < n$ and $y_0 = IV$. Now define MAC=$e_K(y_{n-1})$. Compare the MAC with a MAC generated using CBC encryptions as follows: Take the IV to be 0, then encrypt the sequence $x_1, \ldots, x_n$ to produce the ciphertext sequence $y'_1, \ldots, y'_n$, using $y'_i = e_K(y'_{i-1} \oplus x_i)$, where $1 \leq i < n$ and $y'_0 = IV$. Here the MAC is defined as $MAC' = y'_n$.

i. Prove by mathematical induction that, $y'_n = e_K(y_{n-1})$.

ii. Reason that $MAC = MAC'$.

(c) Suppose that $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is an endomorphic cryptosystem with $\mathcal{P} = \mathcal{C}$=$\{0,1\}^m$. Let $n \geq 2$ be an integer, and define a keyed hash family $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$, where $\mathcal{X}$=$(\{0,1\}^m)^n$ and $\mathcal{Y}$=$\{0,1\}^m$, as follows:

$$h_K(y_1, \ldots, y_n) \quad = \quad e_K(y_1) + 3e_K(y_2) + \ldots + (2n-1)e_K(y_n) \text{mod } 2^m.$$

i. Show that when n is odd, querying the hash output on the input $y_1 = y_2 = \ldots = y_n = y$ reveals the information of $e_K(y)$.

ii. Hence reason that when n is odd, there exists a $(1,1)$ forger for this hash family.

(d) Consider a hash function, $h : \{0,1\}^{1024} \rightarrow \{0,1\}^{128}$ that satisfies the following property:

$$x_1 \equiv x_2 (\text{mod } 2^{32}) \Rightarrow h(x_1) = h(x_2)$$

i. Let Y be a uniformly distributed random element of $\{0, 1, \ldots, 2^{128} - 1\}$. Compute an upper bound on the probability that Y has a preimage.

ii. Given a value $y = h(x)$, show how to take advantage of the above property in order to find a preimage of y. Compute the worst case complexity of the algorithm.

iii. Can we use the above result for performing a second preimage attack? Explain your answer.

iv. Is the above result useful for finding a collision? Explain your answer.

12. Lecture 27-33: Public Key Cryptosystems

(a) Assume that p is an odd prime number. Answer the following questions:

i. Prove that there are exactly $\frac{(p-1)}{2}$ quadratic residues, namely:

$$1^2, 2^2, \ldots, \frac{(p-1)}{2}^2$$

ii. Prove that the product of two quadratic non-residues of p is a quadratic residue of p.

iii. Without using the trial division method how will you decide whether a given number 523 is prime or not? What is the error probability of the test?

(b) A hardware engineer designs a RSA-cryptographic chip with a constant modulus n. However the cryptographer of the company states that this can be potentially harmful: He states that if the message M is communicated to two destinations after encrypting using public keys, e_1 and e_2. Thus, $M^{e_1} \equiv C_1 \bmod (n)$ and $M^{e_2} \equiv C_2 \bmod (n)$.
However if $gcd(e_1, e_2) = 1$, then either the RSA message can be recovered from C_1 and C_2 or the modulus can be factored.

i. Justify that either the multiplicative inverses of C_1 and C_2 exist modulo n, or n can be factored.

ii. If the multiplicative inverses of C_1 and C_2 exist, then the message can be recovered from C_1 and C_2. (**Hint:** Apply Extended Euclidean Algorithm to find integer values, s and t st. $se_1 + te_2 = 1$.)

(c) Let f be a finite function from finite set E to itself and x_0 be a given element of E. The sequence defined by $x_i = f(x_{i-1})$ for $i \in N$ has the shape of the Greek letter ρ, i.e composed of a first part, $x_0, \ldots, x_{q-1}$ (the *tail*) and a second part $x_q, \ldots, x_{q+l-1}$ (the *loop*), such that $x_{q+l} = x_q$. You are provided with two instructions, each costing one unit of time: $Mem(x, S)$ which stores $x \in E$ and S which is any piece of information. The other instruction is $Val(x)$ which gives back for any x the last S value such that (x, S) has been stored or the symbol $\perp$.

i. Propose a simple algorithm which finds for any (f, x_0) the values q, l, x_{q-1} and x_{q+l-1}. What is the average number of f evaluations? What is the average memory size?

ii. Propose a modification of the algorithm that requires a constant size memory. What is the average number of f computations?

(d) Answer the following number theoretic questions:

i. The objective of this question is to find the secret age of a Chinese captain. The only information we know is that one year ago, his age was a multiple of 3, in 2 years it will be a multiple of 5, and in 4 years it will be a multiple of 7. Can you find the age of the captain?

ii. A student has been asked to solve the following problem: Compute the seventh root of 23 in Z_{77}^* by using the Extended Euclidean Algorithm and the Square and multiply algorithm. Help him to get the solution by approaching the problem as follows:

A. Compute d, the inverse of 7 modulus $\phi(77)$, where $\phi(.)$ indicates the Euler's Totient function. Use the extended Euclidean algorithm for this.

B. Compute 23^d modulus 77 using the square and multiply algorithm.

iii. Let $n = p_1 \times p_2 \times \ldots \times p_k$, where $p_1, \ldots, p_k$ are distinct odd primes and an integer $k \geq 2$. The element $a \in Z_n^*$ is said to be a quadratic residue (QR) modulo n if there exists an $x \in Z_n^*$, such that $x^2 \equiv a (\bmod\ n)$. If no such x exists, then a is called a quadratic non-residue (QNR) modulo n.

A. Find the QR and QNR's of Z_{35}^*. How many square roots does each of these QR's have?

B. Prove that an element $a \in Z_n^*$ is a QR modulo n if and only if each component, $(a \bmod p_1, \ldots, a \bmod p_k)$ is a QR of $Z_{p_i}^*$, where $1 \leq i \leq k$.

C. Show that the product of a QR of Z_n^* and QNR of Z_n^* is always a QNR of Z_n^*.

iv. The RSA public key cryptosystem is defined as follows: Let p and q be two prime numbers, let $n = pq$ and $\phi = (p-1)(q-1)$. Select a random integer e with $1 < e < \phi$ such that $gcd(e, \phi) = 1$. Compute d such that $1 < d < \phi$ and $ed \equiv 1 (\bmod\ \phi)$. The public key is (n, e) and the corresponding private key is (n, d). The encryption of a message m is defined as $c = m^e \bmod n$ and the decryption is defined as $m = c^d \bmod n$. Answer the following question regarding RSA:

A. Prove that decryption works.

B. Suppose that Alice and Bob use RSA public keys with the same modulus n, but with different public exponents e_1 and e_2. Prove that Alice can decrypt the messages sent to Bob.

C. Prove that Eve can decrypt a message sent to Bob and Alice if $gcd(e_1, e_2) = 1$. You may use Extended Euclidean Algorithm.

13. Lecture 34-36: Elliptic Curve Cryptosystems

    (a) Let E be the elliptic curve $y^2 = x^3 + x + 28$ defined over Z_{71}.

        i. What is the number of points on the curve?

        ii. Is E a cyclic group?

        iii. What is the maximum order of an element in E?

    (b) Explain the Montgomery Ladder for performing scalar multiplication in Elliptic Curves and show the number of finite field primitives reduce from a conventional double and add algorithm.

14. Lecture 37: Secret Sharing

    (a) Let $n = 4, t = 2, p = 11, s = 3, a_1 = 2$. Construct $a(X)$ in the Shamir's Secret sharing scheme and the shares $y_i, 1 \leq i \leq 4$.

15. Lecture 38-40: Network Security

    (a) Define system and the components of system. Is the statement, *encryption provides system security* correct?

    (b) Explain the Kerberos protocol for key distribution? Explain the functionality of each step.

    (c) How does worms and viruses compare? Describe the components of the virus and how does it protect from anti-virus softwares?

    (d) What is the difference of an Intrusion Detection System (IDS) and firewall?

16. Lecture 41: Side Channel Attack

    (a) What is a Side Channel Attack?

    (b) Explain the working principle of Differential Power Attacks (DPA) and show how can be used to attack cryptosystems. Explain with the help of an example of a block cipher.