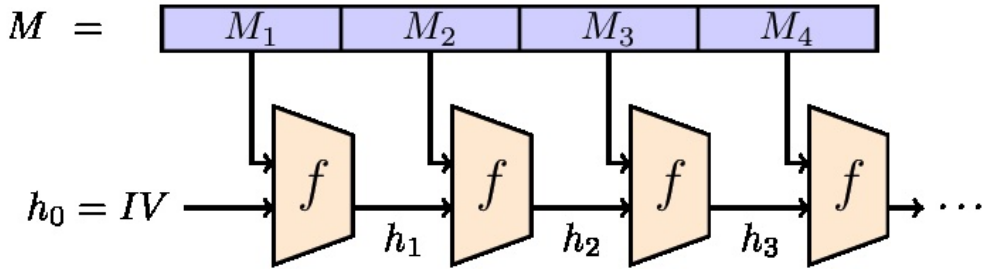
Q1. Describe the notion of Perfect Secrecy and show that the One Time Pad encryption scheme has perfect secrecy.

Q2. Modify the one-time pad encryption scheme where $\mathcal{M} = \mathcal{C} = \{0,1\}^n$, as follows. Let $\mathcal{K} \subset \{0,1\}^n$ and the key generation be such that first a key k' is uniformly chosen from $\{0,1\}^{n/2}$ and then the key is defined by $k = k'||k'$ where $||$ denotes concatenation. Is this scheme perfectly secure? Justify your answer.

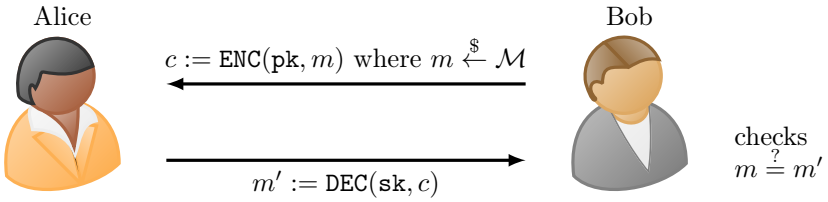
Q3. Appending message length (in blocks) to the end of the message as single block before applying basic CBC-MAC does not result in a secure MAC for arbitrary length messages. Justify this by producing a 5 block message and its valid tag under chosen message attack.

Q4. Let $h : \{0,1\}^\star \to \{0,1\}^n$ be a hash function constructed by iterating a one-way collision resistant compression function f using the Merkle-Damgård construction given in the figure below. The idea is to split the message M into blocks of constant length $M = M_1 \| M_2 \| \dots \| M_t$ (each M_i is typically 512 bits) and to process these blocks along with the intermediate hash values h_1, h_2, h_{t-1} through the compression function f, where IV is the fixed value. The value of h_t is the hash of M and we write $h(M) = h_t$.



Show that defining $\mathbf{MAC}_k(M) = h(k\|M)$ results in an insecure MAC. Assume for simplicity that the key length is the same as the length of the message block $|k| = |M_i|$ and the size of message is multiple of block size.

Q5. [10] Let $\Pi = (\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ be a public key encryption scheme and let $(\texttt{sk}, \texttt{pk})$ be secret key and public key pairs obtained through $\texttt{GEN}$. Alice want to convince Bob, who know the public key $\texttt{pk}$ that she holds the corresponding secret key. It is achieved as follows:



Comment if the above protocol is Zero Knowledge Proof of the fact that Alice owns $\texttt{sk}$, assuming that both Alice and Bob could be malicious.

Q6. State the plain RSA encryption scheme and discuss its correctness.

Q7. Discuss Schnorr identification scheme and it correctness. Convert it into a digital signature scheme using the Fiat-Shamir transform.

Q8. State the Diffie-Hellman key exchange protocol, and ElGamal public key Encryption Scheme and its correctness.

Q9. Comment on the IND-CPA security of the Encrypt-and-Mac authenticated encryption scheme.

Q10. Let N_1, N_2 and N_3 be distinct RSA moduli, such that $\gcd(3, \phi(N_1)) = 1$, $\gcd(3, \phi(N_2)) = 1$ and $\gcd(3, \phi(N_3)) = 1$ and let $e = 3$. Show that given three textbook RSA ciphertexts of a number $m < \min(N_1, N_2, N_3)$ under public keys (N_1, e), (N_2, e) and (N_3, e) respectively, one can quickly find the underlying message m.

Q11. Consider the following private key encryption scheme $\Pi = (\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ with $\mathcal{K} = \mathcal{M} = \{0,1\}^n$ and $\mathcal{C} = \{0,1\}^{n+1}$:

- $k \xleftarrow{\text{uni}} \texttt{GEN}(1^n)$ i.e., $\texttt{GEN}$ generates a uniform key.
- $c := \texttt{ENC}_k(m)$, with $c = (m \oplus k) \Big\| \left(\bigoplus_{i=1}^{|k|} k_i \right)$, where k_i is the i^{th} key bit.
- $\texttt{DEC}_k(c)$ outputs $(c_1 c_2 \dots c_n) \oplus k$, where c_i is the i^{th} bit of ciphertext.

Show that Π is not perfectly secret.

Q12. Let m be a message consisting of ℓ AES blocks (say $\ell = 100$). Alice encrypts m using CBC mode and transmits the resulting ciphertext c to Bob. Due to a hardware error, ciphertext block number $\ell/2$ 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? Justify your answer.

Q13. Suppose Alice shares a secret key encryption key, K_{AB} with Bob, and a different secret key encryption key, K_{AC} with Charlie. Describe a method for Alice to encrypt an m-block message M such that it can only be decrypted with the cooperation of both Bob and Charlie. The ciphertext should only be a constant size greater than m blocks. You may assume that Bob and Charlie have a pre-established secret channel on which to communicate.

Q14. A researcher at IISERB did important research related to the Covid cure and she wishes to get it digitally signed by the director to ensure that she is the original inventor of the algorithm. While getting the document signed, she does not wish to reveal the contents to the director. A protocol that fits in this situation is called a blind signature protocol. In this protocol, if the signer ever sees the document-signature pair, he should not be able to determine when or for whom he signed it, even though he can verify that the signature is valid. Design a blind signature protocol using an RSA-based digital signature scheme and justify its correctness.

Q15. Consider the following variant of the Fiat-Shamir identification protocol: Choose large primes p, q and let $n = pq$. The secret is $x \in \mathbb{Z}_n^*$, and the public id is $y = x^2 \pmod{n}$. The prover randomly selects an odd r, $0 < r < n$ and sends r to the verifier. The Verifier sends a random bit b to the user who replies with $c = x^r \pmod{n}$ if$b = 1$, else replies with $c = y^r \pmod{n}$. The verifier then verifies if $c^{1+b} = y^r \pmod{n}$. Is this protocol secure? Is it zero-knowledge proof? Justify your answers.

Q16. Consider a hash function h given by the following algorithm: Fix a large prime p such that $p - 1$ has a large prime factor q and fix an element g of order q in $\mathbb{Z}_p^*$. On input string x, cut x into blocks $x_1, x_2, \ldots, x_n$ such that each x_i is a number between 1 and q. Let

$$h(x) = \sum_{i=1}^{n} g^{x_i} \pmod{p}$$

Show that h is not secure by designing an efficient algorithm that, on any input u, computes an x_u such that $h(x_u) = u$. If required, you may assume the existance of an efficient algorithm A that, on input $v_i, v_2, \ldots, v_t, u \in \mathbb{Z}_p^*$ with $t = \lceil \log p \rceil$ and $v_i \neq v_j$ for $i \neq j$, computes a polynomial $Q(y_1, y_2, \ldots, y_t)$ that has at most t terms each occuring with coefficient 1 such that

$$Q(y_1, y_2, \ldots, y_t) = u \pmod{p}.$$

Q17. In the AES encryption algorithm, suppose the ShiftRow operation is removed. Design an algorithm to break as many rounds of this system as possible.

Q18. Discuss the Padding Oracle Attack with an example.