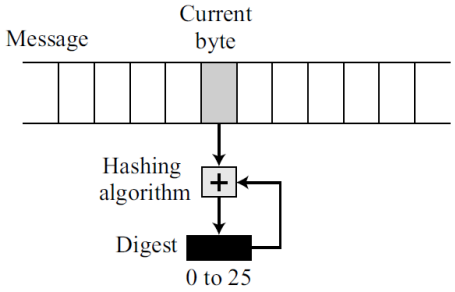
Cryptography (CS-501)
M.Tech (CSE) 1st Year (1st Semester)
Assignment#2

1. Answer the following questions about a family of six people, assuming that the birthdays are uniformly distributed through the days of a week, through the days of a month, through each month of a year, and through the 365 days of the year. Also assume that a year is exactly 365 days and each month is exactly 30 days.
   i. What is the probability that two of the family members have the same birthday? What is the probability that none of them have the same birthday?
   ii. What is the probability that two of the family members are born in the same month? What is the probability that none of them were born in the same month?
   iii. What is the probability that one of the family members is born on the first day of a month?
   iv. What is the probability that three of the family members are born on the same day of the week?

2. In the Random Oracle Model, why does the oracle need to make a note of the digest created for a message and give the same digest for the same message?

3. Distinguish between HMAC and CMAC. Explain why private-public keys cannot be used in creating a MAC.

4. Assume we have a very simple message digest. Our unrealistic message digest is just one number between 0 and 25. The digest is initially set to 0. The cryptographic hash function adds the current value of the digest to the value of the current character (between 0 and 25). Addition is in modulo 26. The following figure shows the idea. What is the value of the digest if the message is "HELLO"? Why is this digest not secure?



5. List the main features of the SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512? In SHA-512, show the value of the length field in hexadecimal for the 10,000 bits of message length and find the number of padding bits for the same length of message.

6. Suppose Alice and Bob use an Elgamal scheme with a common prime $q = 157$ and a primitive root $= 5$.
   i. If Bob has public key $Y_B = 10$ and Alice chose the random integer $= 3$, what is the ciphertext of $M = 9$?

ii. If Alice now chooses a different value of k so that the encoding of $M = 9$ is $C = (25, C_2)$, what is the integer C_2?

7. Describe the general structure of an MD5 hash. How long is the output? How does MD5 handle messages of different lengths? Discuss the security concerns associated with using MD5 for password storage.

8. Using the RSA scheme, let $p = 809, q = 751$, and $d = 23$. Calculate the public key e. Then
   i. Sign and verify a message with $M_1 = 100$. Call the signature S_1.
   ii. Sign and verify a message with $M_2 = 50$. Call the signature S_2.
   iii. Show that if $M = M_1 \times M_1 = 5000$, then $S = S_1 \times S_2$.

9. Do the following:
   i. In the RSA scheme, find the relationship between the size of S and the size of n.
   ii. In the ElGamal scheme, find the size of S_1 and S_2in relation to the size of p.
   iii. In the Schnorr scheme, find the size of S_1 and S_2 in relation to the size of p and q.
   iv. In the DSS scheme, find the size of S_1 and S_2in relation to the size of of p and q.

10. Suppose that the values of p, q, e_1, and r in the Schnorr scheme are the same as the corresponding values in the DSS scheme. Compare the values of S_1 and S_2 in the Schnorr scheme with the corresponding values in the DSS scheme.

11. Show an example of the vulnerability of DSS to selective forgery when the values of p and q are small. Use $p = 29$ and $q = 7$.