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

Q1: Assume we are using one-time pad version of the Vigenère cipher as an encryption technique. In this technique, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 …, then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

i. Encrypt the plaintext "sendmoremoney" with the key stream 9 0 1 7 23 15 21 14 1 11 2 8 9.

ii. Using the ciphertext produced in part a, find a key so that the cipher text decrypts to the plaintext "cashnotneeded".

Q2: Show that DES decryption is, in fact, the inverse of DES encryption.

Q3: Briefly define Group, Abelian group, Ring, Commutative ring and Field.

Q4: For the group $S_n$of all permutations of n distinct symbols,

i. What is the number of elements in S_n?

ii. Show that Sn is not abelian for $n > 2$.

Q5: Given the plaintext $\{000102030405060708090A0B0C0D0E0F\}$ and the key $\{01010101010101010101010101010101\}$,

i. Show the original contents of **State**, displayed as a $4 \ x \ 4$ matrix.

ii. Show the value of **State** after initial AddRoundKey.

iii. Show the value of **State** after SubBytes.

iv. Show the value of **State** after ShiftRows.

v. Show the value of **State** after MixColumns.

Q6: Suppose that p and q are distinct primes, $a^p \equiv a \ (mod \ q)$, and $a^q \equiv a \ (mod \ p)$. Prove that $a^{pq} \equiv a \ (mod \ pq)$.

Q7: Find some primes in the form $5k + 1, 5k + 2, 5k + 3$, and $5k + 4$, where k is a positive integer.

Q8: In ECB mode, bit 17 in ciphertext block 8 is corrupted during transmission. Find the possible corrupted bits in the plaintext.

Q9: Six professors begin courses on Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, respectively, and announce their intentions of lecturing at intervals of $2, 3, 4, 1, 6,$ and 5 days, respectively. The regulations of the university forbid Sunday lectures (so that a Sunday lecture must be omitted). When first will all six professors find themselves compelled to omit a lecture? Hint: Use the CRT.

Q10: What requirements must a public key cryptosystems fulfill to be a secure algorithm? In an RSA system, the public key of a given user is $e = 31, n = 3599$. What is the private key of this user?

Q11: In ElGamal, what happens if $C1$ and $C2$ are swapped during the transition? Assume that Alice uses Bob's ElGamal public key ($e1 = 2$ and $e2 = 8$) to send two messages $P = 17$ and $P' = 37$ using the same random integer $r = 9$. Eve intercepts the ciphertext and somehow she finds the value of $P = 17$. Show how Eve can use a known-plaintext attack to find the value of P'.