Indian Institute of Technology, Delhi

Minor

COL 759 Cryptography and Computer Security

Time: 1 Hour and 30 Minutes Max. Marks 100

Don't ask doubts. Please use your judgement

1. (12 marks) Consider a plaintext message *m* with the first word a 4-letters word and the last letter of the message is not a vowel. The message is encrypted using transposition cipher, as discussed in the class, using a key K (here padding was not required). This encrypted text is further encrypted using Playfair cipher with key "MINEWAS" (now padding was required and 'X' is used for padding).
   Finally, the cipher text obtained is 'QTIYGKTMBSWECMVZCYMEUMECBV'
   Decrypt the ciphertext.

2. (6 marks) Prove that for any positive integer n, $4n \equiv 4 \bmod 12$.

3. (8 marks) Prove that $\gcd(z, xy) = \gcd(z, x)\gcd\left(\frac{z}{\gcd(z,x)}, y\right)$

4. (6 marks) What is the key space of affine cipher with 45 characters?

5. (6 marks) Can Kasiski method, discussed in the class, be used for finding the key length of Hill cipher? Explain.

6. (10 marks) Let $P = \{a, b, c\}$ be set of plaintexts, $C = \{x, y, z\}$ be the set of cipher texts and $K = \{k_1, k_2\}$ be the set of keys.
   The key k_1 maps $a \to z$, $b \to y$, $c \to x$, and key k_2 maps $a \to y$, $b \to z$, $c \to x$.
   Given probabilities to select plaintext a and b be 1/2 and 1/3 respectively. It is also given that in 25% of the cases key k_2 is used.
   Examine the perfect secrecy of the encryption scheme.

7. (8 marks) Consider the following password policy of a system:

   Size of password 5 to 7 character. A character may be a lowercase letter (a-z), an uppercase letter (A-Z) or a digit (0-9) and a password must have at least one digit.

   Now, assume that attacker can crack 2.5×10^6 password in one second with probability of success 0.75. Compute the number of days required in cracking the password.

8. (8 marks) Factorize $n = 589$, given Carmichael function $\lambda(n) = 90$.

9. (8 marks) Prove that if x and y are two integers and their product is coprime with an odd prime q, then at least one of x, y or xy is a quadratic residue modulo q.

10. (10 marks) In RSA cryptosystem, let m be the plaintext and c be its ciphertext i.e., $c = m^e \bmod n$. e is encryption key. If the attacker has computed

$$c^e \bmod n,\ c^{e^2} \bmod n, \cdots,\ c^{e^k} \bmod n, \qquad \text{such that } c^{e^k} \bmod n = c.$$

Can the attacker recover the message *m*? Explain.

11. (8 marks) Prove that the Diophantine equation $x^2 + py + a = 0$ has an integral solution iff the Legendre symbol $(-a/p) = 1$, where *p* is odd prime, and *a* is an integer which is coprime with *p*.

12. (10 marks) In the sieving process, discussed in the class, for factoring large integers using Quadratic Sieve it is required to divide by prime *p* every p^{th} element of array of polynomial Q(*x*) values. Division is highly expensive in comparison to addition/subtraction. Suggest and explain if possible a scheme to replace these divisions by addition or subtraction.