Sardar Vallabhbhai National Institute of Technology, Surat

Course - Intro to Computer Security
Course Code - CO605
Sankita J Patel

MidSem

---

1. **Answer the following:**

   (a) Consider the field $GF(2^4)$. Let field multiplication be performed modulo the irreducible polynomial $x^4 + x + 1$. Compute $(1101)^{-1}$

   (b) A single bit error in exactly one block of ciphertext during transmission. How will this affect the recovery of plaintext in each of the following modes?
   Electronic CodeBook (ECB), CipherBlock Chaining (CBC)

   (c) An old woman goes to the market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number,, but when she had taken them out two at a time, thee was one egg left. The same happened when she picked them out three, four, five and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

   (d) Comment on the security of Digital Signature Standard (DSS) with respect to key-only attack, known-message attack and chosen-message attack.

   (e) Using the Vigenere cipher, encrypt the word "explanation" using the key "leg". What modifications should be done to apply Vernam cipher?

2. **Answer the following (Any three):**

   (a) Suppose two users Alice and Bob have the same RSA modulus n and suppose that their encryption exponents e_A and e_B are relatively prime. Charles wants to send the message m to Alice and Bob; so he encrypts to get $c_A \equiv m^{e_A}(mod n)$ and $c_B \equiv m^{e_B}(mod n)$. Show how Eve can find m if she intercepts c_A and c_B.

   (b) Naive Nelson uses RSA to receive a single ciphertext c, corresponding to the message m. His public modulus is n and his public encryption exponent is e. Since he feels guilty that his system was used only once he agrees to decrypt and ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Evil Eve sends him the ciphertext $2^e c(mod n)$ and gets decrypted ciphertext. Show how this allows Eve to find m.

3. (a) Suppose there are k students in a class. What is the minimum value of k such that the probability of at least two students having the same birthday is 50%?

   (b) How the result derived above can be used to decide security of the hash function?

4. (a) Prove that $60^{-1} mod 101 = 60^{99} mod 101$

   (b) Alice uses three consecutive permutations $[132] \circ [321] \circ [213]$. Which permutation Bob can use to reverse the process? ($\circ$ is the composition operation i.e applying second permutation after the first)

Answers