Indian Institute of Information Technology, Vadodara

Course - Intro to Cryptography
Course Code - CS309
Prof. N Kumar

MidSem

1. Consider a message m containing letter ‘x’ repeated a few hundred of times. Let a cipher is created over m using the following ciphering algorithms. State how an eavesdropper will recognize that the m has one repeated letter. also determine whether or not he can deduce the letter and the key.

   a) Vigenere

   b) Shift cipher

2. An encryption algorithm takes a 64-bit plain-text(say P) and a static 64-bit cipher-text(say C). The encryption algorithm works as follows:
   C = P xor K
   Analyze the security of this cipher against “cipher-text only”, “known plain-text” and “chosen plain-text” attacks. What would be the security strength of this cipher if the algorithm takes a random 64-bit key for each round of encryption.

3. What is the security strength of DES. Double DES considers double encryption two different keys. Does double DES provide more security than DES? Justify answer.

4. What do you mean security of a hash function? Let p be a prime and q be an integer with $p|q$ (i.e., p divides q). Let $H(x) = q^x(modp)$ is a hash function. Explain why (or why not) H(x) is a good hash function.

5. Let a sequence of cipher-text block $< c_1, c_2, \ldots, c_n >$ is computed and sent to the receiver. Assume that one bit in block c_i is corrupted while transmission. Explain how many received blocks will be decrypted incorrectly if ECB, CBC, OFB, CFB or CTR is used for encryption.

> “Cryptography is typically bypassed, not penetrated.”
>
> Adi Shamir

Answers