



JK Lakshmipat University, Jaipur
Institute of Engineering and Technology
Introduction to Cryptography (CS1229)
End Semester Examination, B.Tech., VI Semester

Date: April 22, 2024

Duration: 2.5 hours

MM: 30

There are three questions in this paper with sub-parts. You have to attempt all the questions. The simple calculator and Casio FX-82MS version are allowed in the examination.

1. Explain the following: (1x4 - COs 1,2,3,4)
 - (a) As we know, public-key cryptography can be used for encryption and key exchange. Furthermore, it has some properties (such as non-repudiation) which are not offered by secret-key cryptography. So why do we still use symmetric cryptography in current applications?
 - (b) What is Double Encryption? What is the motivation behind this? Can double encryption be as successful as single encryption? If No, then Why?
 - (c) Why is Modulo 2 Addition a Good Encryption Function?
 - (d) What is the One-Way function? Give an example in the context of Cryptography.
2. Short Answer Questions: (2 x 6 - COs 1, 2, 3,4)
 - (a) If $m = 4$ (m here is number of Flip-Flops), $P_3=P_2=P_1=P_0=1$, What is corresponding LFSR output? What is the maximum period? Design the corresponding LFSR.
 - (b) Encrypt and decrypt by means of the RSA algorithm with the following system parameters: $p = 3, q = 11, d = 7, x = 5$
 - (c) Multiplication in $GF(2^4)$: Compute $A(x).B(x) \bmod P(x)$ in $GF(2^4)$ using the irreducible polynomial $P(x) = x^4 + x + 1$. What is the influence of the choice of the reduction polynomial on the computation?
 1. $A(x) = x^2 + 1, B(x) = x^3 + x^2 + 1$
 2. $A(x) = x^2 + 1, B(x) = x + 1$
 - (d) What is a Cryptographic Attack? What are the broad classifications of attacks? Explain.
 - (e) What is CBC Mode? What is the advantage of CBC mode over ECB Mode? Illustrate the corresponding encryption-decryption figure with the suitable equations.
 - (f) Explain the encryption scheme developed from the Diffie-Hellman key exchange protocol. List out its advantages over standard RSA.

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

Figure 1: Relative Frequency Table

3. Long Answer Questions:

(3+3+4+4 - CO 1, 2, 3, 4,5)

- Using the extended Euclidean algorithm, compute the greatest common divisor and the parameters s, t of 198 and 243.
- We received the following ciphertext, which was encoded with a shift cipher: **xultpajcxitltlxaarpjhtiwtgxktghidhipxcitvgtplpitghlxiwiwtxgqadds**. Perform an attack against the cipher based on a letter frequency count: How many letters do you have to identify through a frequency count to recover the key? What is the cleartext? Note: The standard relative frequency table is given in Figure 1.
- Computing modular exponentiation efficiently is inevitable for the practicability of RSA. Compute the following exponentiations $x^e \bmod m$ applying the square-and-multiply algorithm: $x = 3, e = 197, m = 101$. After every iteration step, show the exponent of the intermediate result in binary notation.
- As we know, the Diffie-Hellman protocol is as secure as the Diffie-Hellman problem, which is probably as hard as the DL problem in the group Z_p^* . However, this only holds for passive attacks, i.e., if Oscar is only capable of eavesdropping. If Oscar (attacker) can manipulate messages between Alice and Bob, the key agreement protocol can easily be broken! Develop an active attack against the Diffie-Hellman key agreement protocol, with Oscar being the man in the middle.