Practice Set

NSS

1. Classify the following violations in terms of Confidentiality, Integrity, Availability and nonrepudiation: (i) A copies B’s homework (ii) A changes B’s signature in a contract
2. Let N denotes an RSA modulus and let ʎ (N) = lcm (p-1, q-1). If e is the encryption exponent, show that decryption exponent can be chosen so that e.d = 1 (mod ʎ (N)).
3. Apply repeated squaring algorithm to compute 325 mod 39.
4. Find the inverse of the polynomial corresponding to 37 H over GF (28). The irreducible polynomial is X8+X4+X3+X+1
5. Suppose Alice, Bob, and Charlie secretly generate a, b and c, respectively, and publish ga mod p, gb mod p, and gc mod p, where p is a prime. Is it possible for Alice, Bob, and Charles each compute gabc mod p as a shared secret known only to the three of them?
6. What is the problem happens if sender uses same random number to encrypt two plaintexts M1 and M2 using Elgamal cryptosystem?
7. Show that if an user choses a prime N as the modulus in the RSA system, it can be trivially broken.
8. Alice wants to send an encrypted message to Bob using RSA, but doesn't know his public Key. So, she sends Bob an email asking for the key. Bob replies with his RSA public key (e, N). However, the active adversary intercepts the message and changes one bit in e from 0 to 1, so Alice receives an email claiming that Bobs public key is (e0, N), where e0 differs from e in one bit. Alice encrypts m with this key and sends it to Bob. Of course, Bob cannot decrypt, since the message was encrypted with the wrong key. So he resends his key and asks Alice to send the encrypted message again, which she does. The adversary eavesdrops to the whole communication without interfering further. Describe how he can recover m.
9. Alice has decided to use RSA for encryption and has generated two large primes p and q and computed N = pq. She has also chosen encryption key eA = 3 and computed her private key dA. When her friend Bob hears about this, he also wants to use RSA. Alice assists him by choosing for him eB = 5 and computing dB using the same N. Alice gives Bob her keys (N; eB) and dB. The next day their common friend Charlie sends message m encrypted to both Alice and Bob, using their respective encryption keys. However, the adversary Deborah eavesdrops and gets hold of the two ciphertext CA and CB. Deborah also notices that Alice and Bob use the same N. Show how Deborah can recover m. You may assume that gcd(m; N) = 1.

Does Deborahs attack generalize to other values of eA and eB than 3 and 5?

1. Consider an Elgamal scheme with common prime **p = 107** and a generator **g = 2**
2. If Alice has public key **=** 94 and Bob chose the random integer **k** = 45 to encrypt message **M** = 60. What will be the ciphertext? How Alice will decrypt it?

Bob now chooses a different value of **k** so that the encoding of M = 60 is **C**= (79, **C2**). Find the value of **C2**.

1. What is differential analysis and Linear analysis of DES. Show with example.
2. Consider Morkle Hellman (MH) public key system with super-increasing secret list a’ = (2, 5, 9, 21, 45, 103, 215, 450, 946) with m = 2003 and w = 1289. Find the public key. Now, show the encryption and decryption of the message (1,0,1,1,1,0,0,1,1). Comment on the security of MH Cryptosystem.
3. A and B are the only two stations on an Ethernet. Each has a steady queue of frames to send. Both A and B attempt to transmit a frame, collide, and A wins the first backoff race. At the end of this successful transmission by A, both A and B attempt to transmit and collide. What is the probability that A wins the second backoff race?
4. **Calculate the efficiency of Slotted Aloha protocol.**  Explain Hidden Terminal Problem. How that is controlled using RTS-CTS scheme.
5. In MACAW protocol, SIFS<PIFS<DIFS. What is the reason behind this ordering?
6. Suppose an active adversary wishes to decrypt a particular message ***c = me (mod n)*** intended for Alice. Assume Alice will decrypt arbitrary cipher-text for adversary other than***c*** itself. Find the procedure adversary will follow to reveal the plaintext message ***m*** corresponding to ***c***from the results provided by Alice.
7. 3 is a popular choice for public key exponent in RSA – Can you reason about it.
8. If a firewall was deployed at IIT Bhubaneswar, would it make the following system less vulnerable to attacks, more vulnerable to attacks, or the same?

* IIT’s academic building, in the context of remote buffer overflow attacks.
* IIT’s web servers, in the context of DDoS attacks.

1. Show mathematically: given a RSA public key (N, e) and the factorization of N, one can derive the secret key d.
2. Find the value of x in the following expression using shank baby step giant step method. 3x ≡ 19 mod 59
3. What RC4 key value will leave S unchanged during initialization? That is, after the initial permutation of S, the entries of S will be equal to the values from 0 through 255 in ascending order.
4. Suppose the round trip propagation delay for a 8 Mbps Ethernet having  
   48-bit jamming signal is 45 μs. What is the minimum frame size?
5. In RC4, if S[2] = 0 and S[1] ≠ 2, then what is the probability of 2nd output be 0. How this can be exploited by adversaries?
6. In DES, Find the output of the initial permutation box when the input is given in hexadecimal as: 0x0002 0000 0000 0001
7. LFSR based stream ciphers are prone to reconstruction attack. Prove/disprove it.
8. State Confusion and Diffusion property of a block cipher. Show any of the two with an example for DES.
9. State 2 week keys of DES. Why are they vulnerable?
10. Let n be an integer. Show that GCD(n2, n2+n+1) = 1
11. How both Authentication and Confidentiality can be achieved using public key (asymmetric key cryptosystems)? Is it good choice to use public key for digital signature?
12. Consider a cipher that has the three keys, three plaintexts and four ciphertext that are represented using the following encryption table

|  |  |  |  |
| --- | --- | --- | --- |
|  | m1 | m2 | m3 |
| k1 | c2 | c3 | c1 |
| k2 | c1 | c2 | c4 |
| k3 | c3 | c1 | c2 |

Suppose that the plaintexts and keys are used with the following probabilities:

f(m1) = f (m2) = 2/7; f(m3) = 3/7

f(k1) = f (k2) = f(k3) = 1/3.

Does the above cryptosystem have perfect secrecy?

1. Compute 518 mod 7 using repeated squaring algorithm
2. Solve following Discrete logarithm using shank baby step giant step algorithm.

3x ≡ 19 mod 59.

1. Apply Miller Rabin Primality Test on n = 397
2. Consider an Elgamal scheme with common prime p = 19 and a generator g = 10. If B has public key Y = 3 and A choose the random integer k = 6, what is the ciphertext for M = 17?
3. In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant αx mod q for some public number α .What would happen if the participants sent each other xα  for some public number instead?

|  |
| --- |
| 1. Write the algorithm to find a given large number is prime or not. 2. Calculate ϕ(n) for n = 1189 where ϕ is Euler totient function. 3. Show that the inverse of 5 (mod 101) is 599 mod 101.Use Formats little theorem |

1. State the size of LFSR used in content scrambling scheme (CSS) for DVD encryption.
2. Let *K* = 111…111 consisting of all 1’s be the key for DES cryptosystem. If DES*K* (*x*) = *y*, then what is DES*K* (*y*)?
3. Select True statements
4. Block Ciphers cannot reuse keys
5. Block cipher and stream cipher behave similar wrt avalanche effect
6. RC4 is used in SSL/TLS
7. Stream Ciphers are slower than Block Ciphers
8. Mail/file transfer use block ciphers
9. Browser/Web Links use block ciphers
10. Block ciphers use more code than stream cipher
11. Prove that OTP with reusing keys doesn’t follow perfect secrecy.