PANIMALAR INSTITUTE OF TECHNOLOGY
Department of Computer Science and Engineering
Academic Year: 2019-2020 (Odd Semester)

INNOVATIVE TOOLS

Degree, Semester& Branch: VII Semester B.E. Computer Science and Engineering
Course Code & Title: CS6701 Cryptography and Network Security
Name of the Faculty member: Dr.V.Subedha, Mrs.S.Hemamalini & Mrs.S.Annie Sheryl

TOPIC: RSA Algorithm **Date: 01.08.2019**

Tit-For-Tat

Tit-For-Tat:

Tit for tat is a game-theory strategy in which each participant mimics the action of their opponent after cooperating in the first round.
Tit for tat can be used in games with repeated moves or in a series of similar games.
Tit for tat emphasizes that cooperation between participants produces a more favorable outcome than a non-cooperative strategy.

When Should Tit-For-Tat Be Used?

- When individuals who have been in competition for a period of time no longer trust one another, the most effective competition reverser is the use of the tit-for-tat strategy.
- Therefore, if the tit-for-tat strategy begins with cooperation, then cooperation ensues. On the other hand, if the other party competes, then the tit-for-tat strategy will lead the alternate party to compete as well.
- Ultimately, each action by the other member is countered with a matching response, competition with competition and cooperation with cooperation.

Outcome:

- Ensures active participation of participants
- Improves comprehensive skill of participants
- Enables participants to analyze and list the given problem statement and solution.

Suggested Activity: Tit-for-Tat

Form two teams A and B.
Instruct Team A to list out the sample out sample test cases which shall effectively bring out weakness of RSA algorithm.
Instruct Team B to implement the algorithm using test cases listed by Team A.
After 5 minutes of discussion, Team A should list out the strengths and Team B should list the weaknesses of the algorithm.
The sample test case worked out by Team A and B could be as follows:

❖ One of sample test case taken by team A can be:

a) Plain text chosen is 12

b) let p=3 and q=5

- ❖ Computation process done by team B can be:

1) n = p*q = 3*5 = 15
2) z(n) = (p-1)(q-1) = 2*4 = 8
3) Choose ‘e’ such that greatest common divisor gcd(8,e) = 1; where 1<e<8
   Therefore ‘e’ chosen as 3
4) select ‘d’ such that d*e = 1 mod 8
   Therefore ‘d’ is chosen as 3 since 3*3 = 1*8 + 1
5) Public Key KU= {e,n} = {3,5}
6) Private Key KR= {d,n} = {3,15}

- ❖ Encryption Process:

Plain Text	:	12
Cipher Text	:	$C = M^e$(mod n)
		$C = 12^3$(mod 15) = 3

- ❖ Decryption Process:

Cipher Text	:	3
Plain Text	:	$M = C^d$(mod n)
		$M = 3^3$(mod 15) = 12

With the above sample test case being worked out followed by 5 minutes of discussion by the teams, strengths and weaknesses of the RSA algorithm can be listed as follows:

- ❖ **Strengths:** Both encryption and decryption in RSA involve raising an integer to an integer power, mod n. this shows there is complexity involved in computation especially when integer values chosen are large. This makes it difficult for the intruder or opponent to recover plaintext from ciphertext.
- ❖ **Weaknesses:**
  - Entire algorithm is based on choosing prime numbers ‘p’ and ‘q’. For small values of ‘p’ and ‘q’ it is very easy to compute and guess ‘e’ and ‘d’ values which are used in computing public key and private key.
  - Factoring ‘n’ into two prime factors is difficult for large values of ‘n’ which is named as factoring problem.
  - Algorithm can be attacked using brute force approach.