CS549: Computer and Network Security
Dept. of CSE, IIT Guwahati

Quiz 1 **Date:** 15-02-2023 **Marks:** 10 **Total Time:** 30 min

Name: **Roll No:**

---

1. Let us consider a Linear Congruential Generator as follows: (2+2+1)=5

   $X_{n+1} = (a\,X_n + c) \bmod 2^4$

   a) What is the maximum period obtainable from the following generator if c =0? Period indicates the number of distinct integers it can generate.
   b) What should be the value of *a* for the above case(s)?
   c) Are there any restrictions required on the seed? If yes, say the restrictions.

(a) $x_{n+1} = a x_n \bmod 16$

So, according to Linear Congruential Generator, we can write $0 < a < 16$ and $0 \leq x_n < 16$ and $0 \leq x_0 < m$ ↑ seed value.

Now, seed value must be an odd number as even number will ~~give~~ generate an integer at some stage which will be divisible by 2^4. So, then onwards the pseudo-random number will be all zero. It means even value is not the good choice.

For the same reason all even values of a are not good choice.

Now let $x_0 = 1$ then, the sequence will be

$a \bmod 16$, $a^2 \bmod 16$, $a^3 \bmod 16$, $a^4 \bmod 16$, ...

So, in this series the same number will be repeated when

$0 < a^n \bmod 2^4 < 2$ i.e. $a^n \bmod 16 = 1$

Lets check,

$a = 1$, → all are 1 → not good

$a = 3$ → 3, 9, 11, 1 → So, period = 4

$a = 5$ → 5, 9, 13, 1 → So, period = 4

$a = 7$ → 7, 1 → So period = 2

$a = 9$ → 9, 1 → So period = 2

$a = 11$ → 11, 9, 3, 1 → So period = 4

$a = 13$ → 13, 9, 5, 1 → So period = 4

$a = 15$ → 15, 1 → So, period = 2

So, Maximum attainable period = 4, marks 2

The values of a are 3 or 5 or 11 or 13. mark 2

Seed must be an odd value. marks 1

2. The problem illustrates a simple application of the chosen ciphertext attack. Bob intercepts a ciphertext C intended for Alice and encrypted with Alice's public key e. Bob want to obtain the original message $M = C^d \bmod n$. Bob chooses a random value r less than n and computes the following:

$Z = r^e \bmod n$

$X = ZC \bmod n$

$T = r^{-1} \bmod n$

Next, Bob gets Alice to authenticate (sign) X with her private key d, thereby decrypting X. Alice returns $Y = X^d \bmod n$. Can the Bob determine M using the information available to him? If yes, show the steps how Bob can determine M. (1+1+3)=5

mark 1 (say Yes)

According to the basic assumption of RSA algo, e and n are known to Bob.

Because, $Z = r^e \bmod n$, we can write $r = Z^d \bmod n$.

But, d is unknown to Bob as it is the private key of Alice.

Now, Let's do the ~~oper~~ following operations (by Bob).

$TY \bmod n$ ← writing this equation give 1 mark.

$\Rightarrow ((r^{-1} \bmod n)(X^d \bmod n)) \bmod n$

using modular arithmetic

$\Rightarrow r^{-1} X^d \bmod n$

$\Rightarrow r^{-1} (ZC \bmod n)^d \bmod n$ ← by replacing X

$\Rightarrow r^{-1} Z^d C^d \bmod n$

for this full proof give 3 marks.

$\Rightarrow$ ~~[illegible]~~

$\Rightarrow (r^{-1} (Z^d \bmod n) C^d) \bmod n$

$\Rightarrow (r^{-1} r C^d) \bmod n$

$\Rightarrow C^d \bmod n$

$\Rightarrow M$

So, yes ~~[illegible]~~, Bob can retrive M by doing a simple operation $TY \bmod n$ for which the private key of Alice is not required.