

Complex

Department of CSE(HONORS)

CRYPTANALYSIS & CYBER DEFENSE 21CS304IRA

Topic:

Types of Pseudorandom Number, Generators

Session - I I

Simple

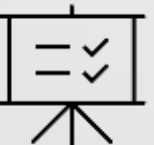
Experiential Learning
(site visits)
Forum Theater
Jigsaw Discussion
Inquiry Learning
Role Playing
Active Review Sessions
(Games or Simulations)
Interactive Lecture
Hands-on Technology
Case Studies
Brainstorming
Groups Evaluations
Peer Review
Informal Groups
Triad Groups
Large Group Discussion
Think-Pair-Share
Writing
(Minute Paper)
Self-assessment
Pause for reflection

AIM OF THE SESSION




To make the students understand with the basic concepts of Pseudorandom Number Generation and its Principles.

INSTRUCTIONAL OBJECTIVES



The objective of this session is to introduces types of Psuedorandom Number Generators

LEARNING OUTCOMES



At the end of this session, students are expected to know

1. Demonstrate types of Random Number Generators.
2. Apply Psuedorandom Number Generators

This module demonstrates block cipher modes of operation. It also helps to identify which ciphers operate as block ciphers and stream ciphers. Principles of Pseudorandom Number Generators are listed and types of Pseudorandom Number Generators are discussed. Finally, Stream Ciphers and its example RC4 algorithm are demonstrated.

A pseudorandom number generator (PRNG) is a deterministic algorithm that produces a sequence of numbers that appear to be random but are actually generated using a mathematical formula. PRNGs are widely used in cryptography, simulations, and other applications where random numbers are required.

SESSION DESCRIPTION

- It is important to note that while PRNGs can produce numbers that appear random, they are not truly random and are subject to certain vulnerabilities.
- For example, if an attacker can determine the seed value and the algorithm used by a PRNG, they may be able to predict the entire sequence of numbers it will produce.
- To address these vulnerabilities, cryptographic PRNGs use a combination of a secret key and a seed value to produce a sequence of numbers that is both random and unpredictable.
- These cryptographic PRNGs are used in applications such as generating encryption keys, authentication tokens, and random numbers for use in cryptographic protocols.

SESSION DESCRIPTION

Types of Pseudorandom Number Generator (PRNGs)

Linear Congruential Generator (LCG):

A Linear Congruential Generator (LCG) is a type of pseudorandom number generator (PRNG) that generates a sequence of random numbers based on a linear equation. It follows the recurrence relation:

$$X_{n+1} = (a * X_n + c) \bmod m$$

where:

X_n is the current state or the previously generated number in the sequence.

a , c , and m are constants chosen for the LCG algorithm.

The mod m operation calculates the remainder when $(a * X_n + c)$ is divided by m .

SESSION DESCRIPTION

Types of Pseudorandom Number Generator (PRNGs)

- The LCG algorithm starts with an initial seed value (X_0) and uses the recurrence relation to generate subsequent numbers in the sequence. Each new number is obtained by multiplying the previous number by a constant, adding another constant, and then taking the modulo of the result.
- The generated numbers are considered pseudorandom because they appear to be random, but they are actually determined entirely by the initial seed value and the chosen constants. The quality of randomness in an LCG depends on the values of a , c , and m . With carefully chosen constants, LCGs can produce a long period of seemingly random numbers before the sequence repeats.

SESSION DESCRIPTION

Types of Pseudorandom Number Generator (PRNGs)

- However, LCGs have limitations and weaknesses. If poorly chosen constants are used, the generated sequence may exhibit patterns or have a short period, making it predictable. LCGs are not suitable for cryptographic applications that require high-quality random numbers due to their deterministic nature and vulnerability to attacks.
- To improve the randomness and security of LCGs, it is recommended to carefully select the constants and periodically reseed the generator with a high-quality random source. In modern applications, more advanced random number generators, such as cryptographic random number generators (CSPRNGs), are preferred as they offer better randomness and stronger security guarantees.

SESSION DESCRIPTION

Types of Pseudorandom Number Generator (PRNGs)

Blum Blum Shub Generator (BBS):

The Blum Blum Shub (BBS) generator is a cryptographic pseudorandom number generator (CPRNG) that was introduced by Lenore Blum, Manuel Blum, and Michael Shub in 1986. It is designed to generate random numbers based on the quadratic residues modulo a Blum integer. The BBS generator is considered secure, relying on the assumption that the integer factorization problem is computationally difficult.

SESSION DESCRIPTION

Types of Pseudorandom Number Generator (PRNGs)

Here's how the BBS generator works:

Key Generation:

Two large prime numbers, p and q , are chosen such that $p \equiv q \equiv 3 \pmod{4}$. These primes are kept secret and are typically of equal length to enhance security.

The Blum integer, n , is calculated as the product of p and q , which serves as the modulus for the generator.

SESSION DESCRIPTION

Types of Pseudorandom Number Generator (PRNGs)

Seed Generation:

A seed value, X_0 , is selected, which should be relatively prime to n . It is advisable to use a seed generated from a high entropy source to ensure randomness.

Random Number Generation:

Each random bit or byte is generated through the following steps:

Compute $X_{i+1} = (X_i)^2 \bmod n$, where X_i represents the previously generated value.

The least significant bit or byte of X_{i+1} is extracted and used as the random output.

SESSION DESCRIPTION

Types of Pseudorandom Number Generator (PRNGs)

- The BBS generator generates a sequence of random bits or bytes by repeatedly squaring the previous value and taking the modulo n . The resulting output is the least significant bit or byte, depending on the desired output size.
- The security of the BBS generator relies on the difficulty of factoring the Blum integer n into its prime factors. If an attacker can efficiently factorize n , it would enable them to predict future outputs of the generator. Thus, the security of the BBS generator hinges on the secrecy of the prime numbers p and q .

SESSION DESCRIPTION

Types of Pseudorandom Number Generator (PRNGs)

Although the BBS generator is known for its simplicity and ease of implementation, it tends to be slower compared to other pseudorandom number generators due to the modular exponentiation operation involved. As a result, it is commonly used in applications where security is prioritized over speed, such as cryptographic key generation.

SELF-ASSESSMENT QUESTIONS

1. The LCG equation is defined as $X_{n+1} = (a * X_n + c) \text{ mod } m$. What does "mod" represent in this equation?

- a) Modulus operation
- b) Multiplication operation
- c) Addition operation
- d) Exponentiation operation

2. Which of the following is a potential drawback of using an LCG?

- a) Short period length
- b) Poor statistical properties
- c) Predictability of the generated sequence
- d) All of the above

SELF-ASSESSMENT QUESTIONS

3. Which of the following is an essential component of the Linear Congruential Generator (LCG)?

- a) Seed value
- b) Modulus
- c) Multiplier
- d) All of the above

4. In an LCG, the seed value:

- a) Determines the length of the generated sequence
- b) Determines the period of the generated sequence
- c) Determines the initial state of the generator
- d) None of the above

SUMMARY

This session provides an overview of the topics typically covered in a course on PRNGs. The duration and depth of each topic may vary depending on the level and intended audience of the course. Additionally, practical exercises, assignments, and assessments can be incorporated throughout the course to reinforce learning and practical application of PRNG concepts.

TERMINAL QUESTIONS

1. Suppose an LCG is defined with the parameters:

$$a = 7$$

$$c = 0$$

$$m = 10$$

Find the seed value (X_0) that produces the longest possible period for this LCG.

2. An LCG has the following parameters:

$$a = 25214903917$$

$$c = 11$$

$$m = 2^{48}$$

If the initial seed (X_0) is 7, calculate the 10th number generated by the LCG.

3. Suppose a BBS generator is initialized with the following parameters:

$$p = 103$$

$$q = 107$$

$$X_0 = 33$$

Calculate the next 10 bytes generated by the BBS generator.

4. Consider a BBS generator with the following parameters:

$$p = 17$$

$$q = 29$$

$$X_0 = 2$$

Determine whether the BBS generator will produce a full period or a shorter period, and explain your reasoning.

REFERENCES FOR FURTHER LEARNING OF THE SESSION

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015.
3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011
4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

THANK YOU



Team – CACD