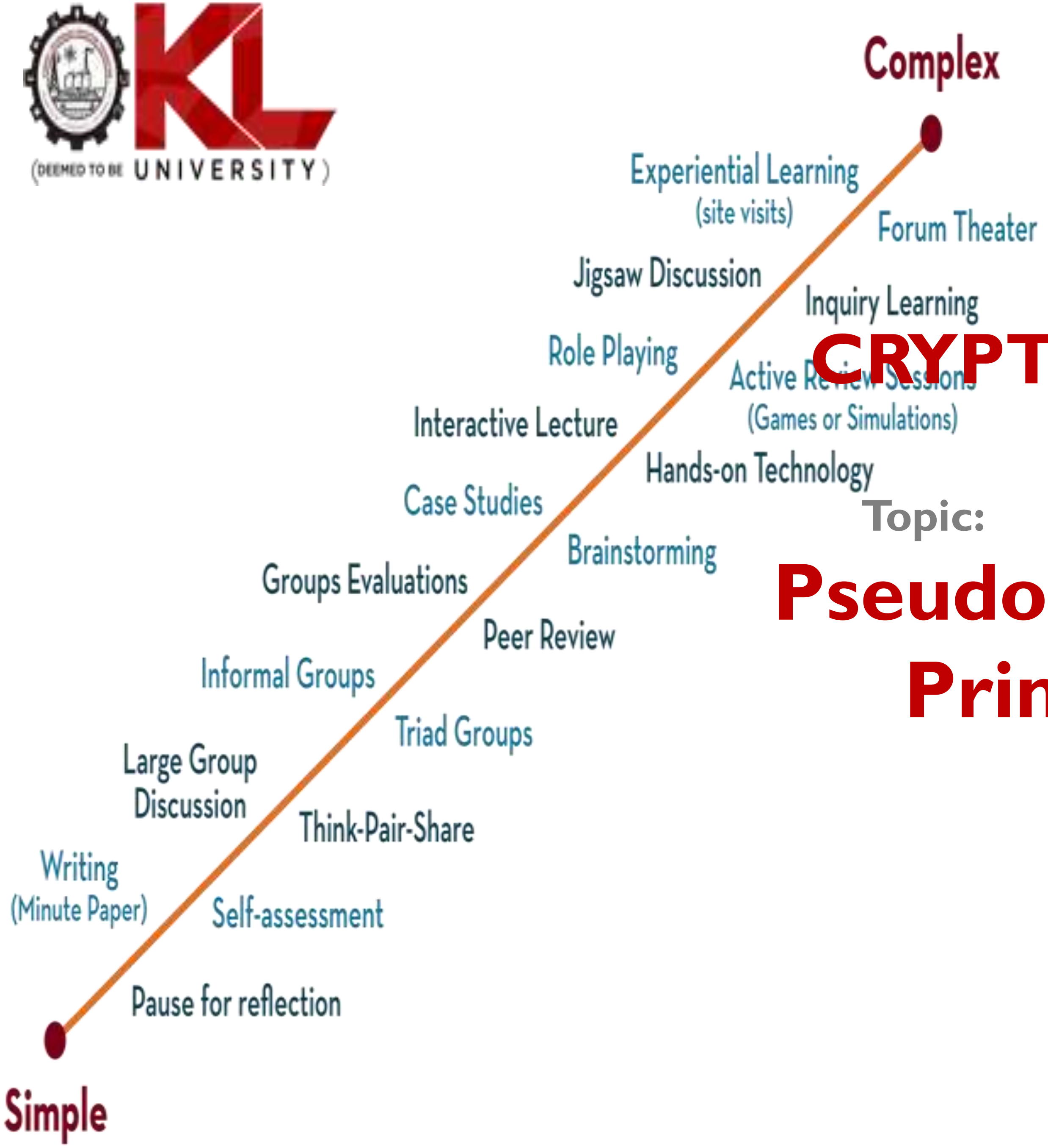
Department of CSE(HONORS)

CRYPTANALYSIS & CYBER DEFENSE 21CS3041RA

Topic:

Pseudorandom Number Generation Principles and Pseudorandom Number, Generators

Session -10



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 introduce the basic principles of Random Number Generation and types of Random Number Generators.

LEARNING OUTCOMES

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

1. List principles of Random Number Generation
2. Demonstrate types of Random Number Generators

Module Description

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.

SESSION INTRODUCTION

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

Pseudorandom Number Generation

Random Numbers

A random number is a value that is generated unpredictably and lacks any discernible pattern or relationship to previously generated values. Random numbers play a crucial role in various fields, including cryptography, simulations, statistical analysis, gaming, and more.

SESSION DESCRIPTION

Types of Random Numbers:

True Random Numbers (TRNG):

- True random numbers are generated from unpredictable physical processes, such as atmospheric noise, radioactive decay, or thermal noise.
- TRNGs provide genuinely random and unbiased numbers, as they are derived from natural phenomena.
- However, generating true random numbers can be challenging and often requires specialized hardware.

SESSION DESCRIPTION

Types of Random Numbers:

Pseudorandom Numbers (PRNG):

- Pseudorandom numbers are generated by deterministic algorithms that use mathematical formulas and a seed value to produce a sequence of numbers that appears random.
- PRNGs are repeatable, meaning that with the same seed value, they will produce the same sequence of numbers.
- However, the generated numbers are not truly random, but rather exhibit statistical randomness and pass various tests for randomness.

SESSION DESCRIPTION

Pseudorandom Number Generation

Criteria:

1.Uniform distribution: The distribution of bits in the sequence should be uniform.

2.Independence: No one subsequence in the sequence can be inferred from the others.

SESSION DESCRIPTION

Pseudorandom Number Generation

Application of Random Numbers:

Random numbers find applications in various areas, such as

- Generating encryption keys
- Conducting statistical sampling
- Simulating real-world scenarios
- Ensuring fairness in games
- Enhancing security in cryptographic systems.

SESSION DESCRIPTION

Pseudorandom Number Generation

Types of Random Numbers (IN DETAIL):

□True Random Number Generators (TRNGs):

True Random Number Generators (TRNGs) are devices or algorithms that generate random numbers from unpredictable physical processes or phenomena. Unlike pseudorandom number generators (PRNGs), which rely on deterministic algorithms, TRNGs utilize inherent randomness in the physical world to produce truly random and unbiased numbers.

SESSION DESCRIPTION

Pseudorandom Number Generation

Here are some key points about TRNGs:

□ **Unpredictable Sources**: TRNGs extract randomness from various sources, such as atmospheric noise, radioactive decay, thermal noise, electronic noise, or even quantum phenomena. These sources are considered unpredictable and provide a source of true randomness.

□ **Hardware-based TRNGs**: Hardware-based TRNGs use physical components or circuits to capture random physical processes. They can include sensors, amplifiers, analog-to-digital converters, and post-processing modules to refine the obtained raw random data.

□ **Physical Phenomena**: TRNGs exploit physical phenomena that exhibit inherent randomness, such as variations in voltage, temperature, or radioactive decay events. These phenomena provide a basis for generating random bits.

SESSION DESCRIPTION

Pseudorandom Number Generation

□ Testing and Certification: TRNGs undergo rigorous testing and evaluation to verify their random properties and ensure they meet specific standards. Organizations like the National Institute of Standards and Technology (NIST) provide guidelines and certification processes for TRNGs.

□ Non-deterministic Output: TRNGs generate numbers that are not derived from any algorithmic or mathematical formula. The output of a TRNG at a given moment is not dependent on previous outputs or the current state of the device.

□ Applications: TRNGs are essential in applications where true randomness is critical, such as cryptography, key generation, gambling, lotteries, and scientific simulations. They provide a high level of security and eliminate the predictability associated with pseudorandom numbers.

SESSION DESCRIPTION

Pseudorandom Number Generation

- It's worth noting that TRNGs may have limitations, such as slower generation speeds compared to PRNGs and potential biases or correlations in the generated random numbers.
- Thus, careful design, post-processing techniques, and statistical analysis are employed to ensure the quality and reliability of the generated random numbers.

SESSION DESCRIPTION

Pseudorandom Number Generation

- □ Pseudorandom Number Generators (PRNGs):

Pseudorandom Number Generators (PRNGs) are algorithms or software routines that generate sequences of numbers that appear to be random, but are actually determined by a deterministic process. PRNGs use mathematical formulas and an initial seed value to produce a sequence of numbers that exhibits statistical randomness properties

SESSION DESCRIPTION

Pseudorandom Number Generation

Here are some key points about PRNGs:

□ Deterministic Algorithms: PRNGs use deterministic algorithms to generate random-like sequences. Given the same seed value, a PRNG will produce the same sequence of numbers. The output is entirely determined by the algorithm and the seed value.

□ Seed Value: The seed value serves as the initial input to the PRNG algorithm.

By changing the seed value, different sequences of numbers can be generated. If the same seed value is used, the same sequence will be produced.

□ Periodicity: PRNGs have a period, which is the length of the sequence before it repeats itself. The period is determined by the algorithm and the internal state of the PRNG. A good PRNG should have a long period to avoid predictability and repetition.

SESSION DESCRIPTION

Pseudorandom Number Generation

□Reproducibility: PRNGs offer reproducibility, meaning that given the same seed value, the sequence of numbers can be replicated. This property is useful in simulations, testing, and debugging scenarios.

□Statistical Randomness: PRNGs strive to generate sequences that exhibit statistical randomness properties, such as uniform distribution, independence, and Unpredictability. They are designed to pass various statistical tests for randomness.

□Cryptographically Secure PRNGs (CSPRNGs): In cryptographic applications, special PRNGs called Cryptographically Secure PRNGs (CSPRNGs) are used. CSPRNGs are designed to withstand cryptographic attacks and provide a high level of randomness suitable for encryption, key generation, and other security-sensitive operations.

□Efficiency: PRNGs are computationally efficient and can generate a large number of random-like sequences quickly. They are commonly used in applications like simulations, gaming, numerical analysis, and modeling.

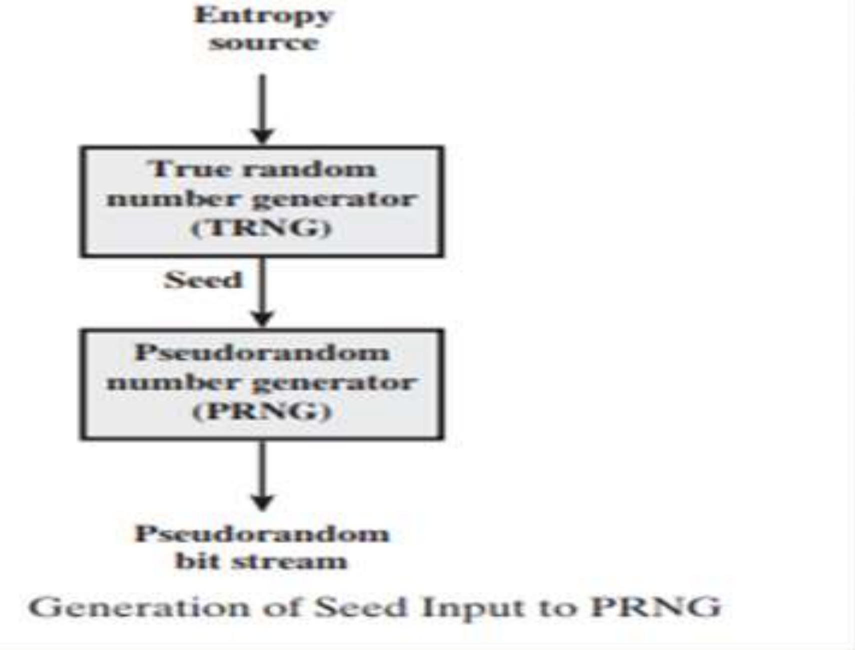
SESSION DESCRIPTION

Pseudorandom Number Generation

- It's important to note that PRNGs, unlike true random number generators (TRNGs), are not inherently random.
- They rely on their algorithmic design and the seed value for their randomness.
- As a result, PRNGs may exhibit patterns or correlations in their output over long periods or if the seed values are not chosen carefully.

SESSION DESCRIPTION

Pseudorandom Number Generation


Entropy source
True random number generator (TRNG)
Seed
Pseudorandom number generator (PRNG)
Pseudorandom bit stream
Generation of Seed Input to PRNG

Generation of Seed Input to PRNG
Copyrights of this diagram are reserved with original author

SESSION DESCRIPTION

Pseudorandom Number Generation

□ Pseudo-Random Function (PRF)

A Pseudo-Random Function (PRF) is a deterministic function that takes an input key and an input message or data and produces an output that appears random and unpredictable, even though it is computed by a deterministic algorithm. PRFs are commonly used in cryptography for various purposes, including key generation, data integrity verification, message authentication codes (MACs), and pseudorandom number generation.

SESSION DESCRIPTION

Pseudorandom Number Generation

Here are some key points about PRFs:

□ **Deterministic Function:** A PRF is a deterministic function, meaning that given the same input key and message, it will always produce the same output. This property allows for reproducibility and consistency in cryptographic operations.

□ **Pseudo randomness:** PRFs generate output that exhibits pseudorandomness, meaning that the output appears random and unpredictable to an observer who does not have knowledge of the key. However, since the output is computed by an algorithm, it is not truly random.

□ **Keyed Function:** PRFs rely on a secret key that is known only to the parties involved in the cryptographic operation. The key enhances the security of the PRF and ensures that the output is dependent on both the input message and the key.

SESSION DESCRIPTION

Pseudorandom Number Generation

□ Security Properties: A secure PRF should exhibit properties like unpredictability, resistance to key recovery, and computational indistinguishability. These properties ensure that an adversary cannot distinguish the output of the PRF from truly random output or gain knowledge of the key based on the observed output.

□ PRF vs. PRNG: While both PRFs and Pseudorandom Number Generators (PRNGs) generate pseudorandom output, PRFs are typically designed for specific cryptographic purposes, such as generating keys or providing integrity and authentication, whereas PRNGs are focused on generating random-like sequences of numbers for general-purpose applications.

SESSION DESCRIPTION

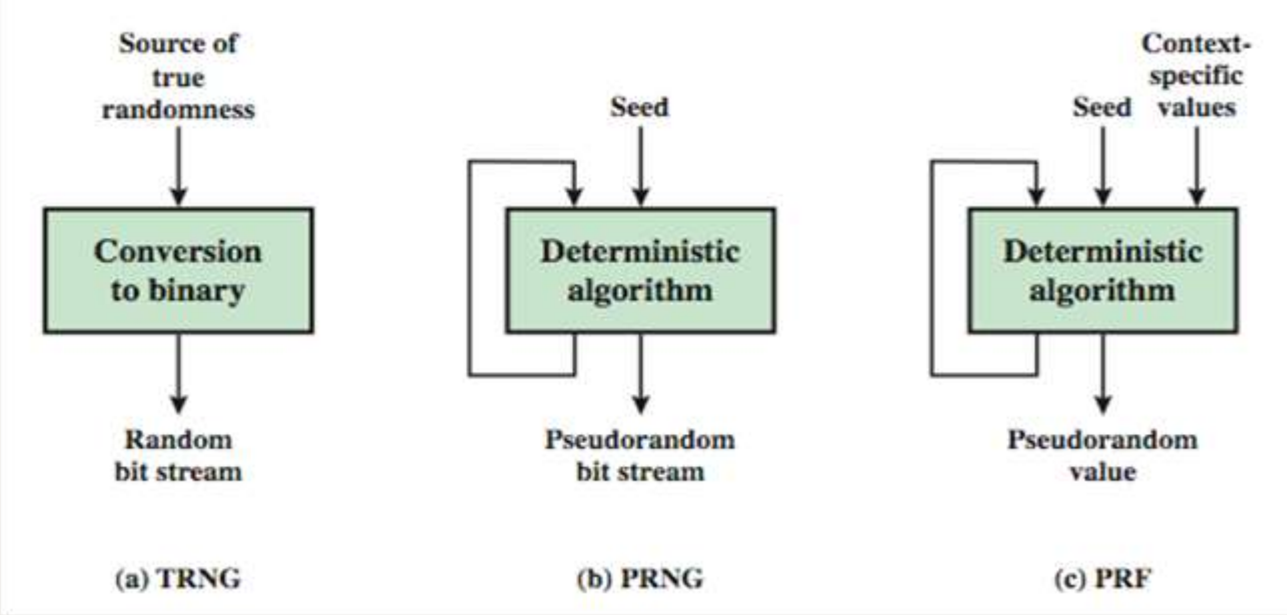
Pseudorandom Number Generation

- □ Common PRF Constructions: HMAC (Hash-based Message Authentication Code) is a widely used construction for PRFs. It combines a cryptographic hash function with a secret key to produce a pseudorandom output. Other constructions, such as block ciphers in various modes, can also serve as PRFs.

- □ PRFs play a crucial role in ensuring the security and integrity of cryptographic systems. They are fundamental building blocks for many cryptographic protocols and applications, providing the necessary pseudo randomness and security properties required for secure communications and data protection.

SESSION DESCRIPTION

Pseudorandom Number Generation



Schematic diagram of TRNG, PRNG and PRF.
Copyrights of this diagram are reserved with original author

SELF-ASSESSMENT QUESTIONS

1.Which of the following statements is true about random number generators (RNGs)?

a) RNGs generate truly random numbers.

b) RNGs generate predictable sequences of numbers.

c) RNGs require a seed value to generate random numbers.

d) RNGs are not used in cryptography.

2. What is the main purpose of a random number generator in cryptography?

a) To generate random keys for encryption algorithms.
b) To generate random plaintext messages.
c) To generate random ciphertext messages.
d) To generate random IVs for cryptographic modes of operation.

SELF-ASSESSMENT QUESTIONS

3. Which of the following is a key principle of a secure random number generator?

a) Determinism

b) Predictability

c) Reproducibility

d) Unpredictability

4. Which type of random number generator uses physical phenomena to generate randomness?

a) Pseudorandom number generator (PRNG)
b) Hardware random number generator (HRNG)
c) Deterministic random bit generator (DRBG)
d) Software-based random number generator

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. Summarize PRNG concepts
2. Illustrate TRNG with neat diagram.
3. Demonstrate PRNG with neat diagram.
4. Illustrate PRF with neat diagram.

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, Algorthms, 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