

Complex

Department of CSE(HONORS)

CRYPTANALYSIS & CYBER DEFENSE 2ICS304IRA

Topic:

Types of Pseudorandom Number, Generators

Session - I2

Simple

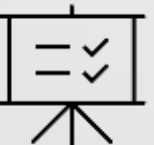
Experiential Learning
(site visits)
Forum Theater
Jigsaw Discussion
Inquiry Learning
Role Playing
Active Review Sessions
(Games or Simulations)
Interactive Lecture
Hands-on Technology
Case Studies
Brainstorming
Groups Evaluations
Peer Review
Informal Groups
Triad Groups
Large Group Discussion
Think-Pair-Share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

AIM OF THE SESSION




To make the students understand 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

- Demonstrate Psuedorandom Number Generators using Block Ciphers.
- Demonstrate X9.17 ANSI Ring

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

PRNG Using Block Cipher Modes of Operation

- The Output Feedback (OFB) mode is recommended in standards such as X9.82 and RFC 4086.
- Figure 12.1 provides an illustration of the two methods used in OFB mode. In both methods, the seed consists of two components: the encryption key and a value that undergoes updates after generating each block of pseudorandom numbers.
- For instance, when using AES-128, the seed comprises a 128-bit key and a 128-bit value.

SESSION DESCRIPTION

PRNG Using Block Cipher Modes of Operation

In the Counter (CTR) case, the value is incremented by 1 after each encryption operation. On the other hand, in the OFB case, the value is updated to be equal to the value of the preceding pseudorandom number generator (PRNG) block.

In both scenarios, pseudorandom bits are generated one block at a time. For example, with AES, the PRNG bits are generated in chunks of 128 bits at a time.

It is important to note that the above information is based on the mentioned standards and the specific mode of operation being discussed.

SESSION DESCRIPTION

PRNG Using Block Cipher Modes of Operation

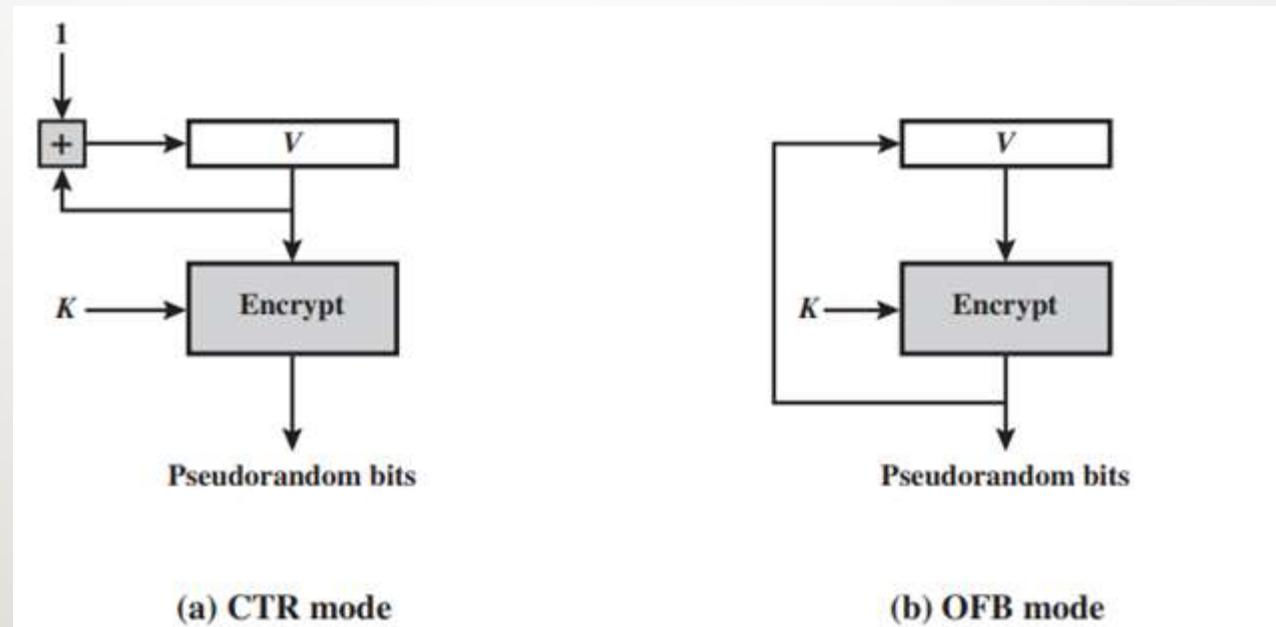


Figure 12.1: PRNG Mechanism Based on Block ciphers
Copyrights of this diagram are reserved for the original author

SESSION DESCRIPTION

ANSI Ring X9.17

The ANSI X9.17 standard specifies a PRNG that is considered to be one of the strongest in terms of cryptographic security. This technique is utilized in various applications, including financial security and PGP

Figure 12.2 provides a depiction of the algorithm employed in this PRNG, which utilizes triple DES for encryption.

The algorithm relies on two pseudorandom inputs as its driving force. The first input is a 64-bit representation of the current date and time, which is updated each time a number is generated. The second input is a 64-bit seed value that is initially set to an arbitrary value and subsequently updated during the generation process.

SESSION DESCRIPTION

ANSI Ring X9.17

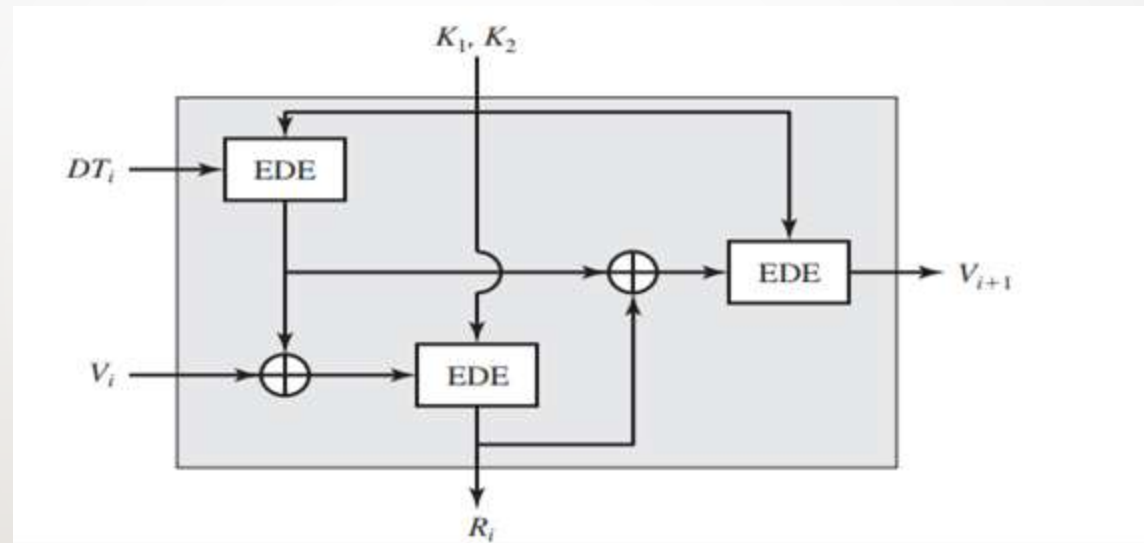


Figure 12.2: ANSI X9.17 Pseudorandom Number Generator
Copyrights of this diagram are reserved for the original author

SESSION DESCRIPTION

ANSI Ring X9.17

Key Usage: The PRNG utilizes three triple DES encryption modules, with each module employing the same pair of 56-bit secret keys. These keys are specifically designated for pseudorandom number generation purposes and should remain confidential.

- **Output Format:** The PRNG generates a 64-bit pseudorandom number as its primary output. Additionally, it produces a 64-bit seed value, which is an essential component for the subsequent generation of pseudorandom numbers.

SESSION DESCRIPTION

ANSI Ring X9.17

Let us define the following quantities.

DT_i	Date/time value at the beginning of i th generation stage
V_i	Seed value at the beginning of i th generation stage
R_i	Pseudorandom number produced by the i th generation stage
K_1, K_2	DES keys used for each stage

Then

$$R_i = \text{EDE}([K_1, K_2], [V_i \oplus \text{EDE}([K_1, K_2], DT_i)])$$
$$V_{i+1} = \text{EDE}([K_1, K_2], [R_i \oplus \text{EDE}([K_1, K_2], DT_i)])$$

where $\text{EDE}([K_1, K_2], X)$ refers to the sequence encrypt-decrypt-encrypt using two-key triple DES to encrypt X .

Figure 12.3: ANSI X9.17 Psuedorandom Number Generator Equations
Copyrights of this diagram are reserved for the original author

SESSION DESCRIPTION

- Several factors contribute to the cryptographic strength of this method. The technique utilizes a 112-bit key, which ensures a high level of security. The process involves three EDE (Encrypt-Decrypt-Encrypt) encryptions, which effectively amounts to a total of nine DES (Data Encryption Standard) encryptions. This multiple encryption scheme enhances the overall security of the method.
- The generation process of pseudorandom numbers is driven by two inputs: the current date and time value and a seed value. It is important to note that the seed value is distinct from the pseudorandom number generated by the generator. This separation of inputs adds an additional layer of complexity to the system and makes it extremely challenging for an adversary to compromise the security.

SESSION DESCRIPTION

- The generation process of pseudorandom numbers is driven by two inputs: the current date and time value and a seed value. It is important to note that the seed value is distinct from the pseudorandom number generated by the generator. This separation of inputs adds an additional layer of complexity to the system and makes it extremely challenging for an adversary to compromise the security.

SESSION DESCRIPTION

- Even if a pseudorandom number were to be compromised, it would be infeasible for an attacker to deduce the original seed value or the encryption key. This is due to the utilization of an additional EDE operation in the generation process, which further obscures the relationship between the seed value and the pseudorandom number.
- The combination of a large key size, multiple encryptions, separate inputs, and additional encryption steps ensures that the level of material that an adversary would need to compromise is overwhelmingly large. This makes the method highly resistant to attacks and provides a strong cryptographic foundation for generating pseudorandom numbers.

SELF-ASSESSMENT QUESTIONS

1. Which of the following is a block cipher mode of operation commonly used for pseudorandom number generation?

- a) ECB (Electronic Codebook)
- b) CTR (Counter)
- c) CBC (Cipher Block Chaining)
- d) OFB (Output Feedback)

2. Which property makes block cipher modes of operation suitable for pseudorandom number generation?

- a) Randomness
- b) Determinism
- c) Key expansion
- d) Block size

SELF-ASSESSMENT QUESTIONS

3. In which block cipher mode of operation is the previous ciphertext block (or initialization vector) encrypted to generate the pseudorandom keystream?

- a) ECB (Electronic Codebook)
- b) CBC (Cipher Block Chaining)
- c) CTR (Counter)
- d) OFB (Output Feedback)

4. Which block cipher mode of operation allows for parallel encryption and decryption of individual blocks?

- a) ECB (Electronic Codebook)
- b) CTR (Counter)
- c) CBC (Cipher Block Chaining)
- d) OFB (Output Feedback)

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 the concept of pseudorandom number generation using block cipher modes of operation.
2. Identify the purpose of using block cipher modes of operation for pseudorandom number generation.
3. Summarize the role of the initialization vector (IV) in block cipher modes of operation for pseudorandom number generation.
4. Enumerate the potential security vulnerabilities and weaknesses associated with using block cipher modes of operation for pseudorandom number generation.
5. Identify the impact of the block size on the efficiency and security of pseudorandom number generation using block cipher modes of operation.

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