Cryptographics Algorithms

Reading

35m

✔ Status | Incomplete

Introduction

This reading focuses on Canadian regulations for cryptographic algorithms and their importance for new cybersecurity professionals. As a cybersecurity professional in Canada, it is essential to understand the legal and regulatory requirements governing the use of cryptographic algorithms. Cryptography plays a vital role in protecting sensitive data and securing network communications, and understanding the regulatory landscape is critical to ensuring compliance and avoiding legal consequences. By reviewing these regulations, you will have a solid foundation for understanding the legal and compliance aspects of cryptography in Canada, ensuring that your organization's cryptographic practices align with industry standards and regulations.

Canadian Centre for Cyber Security

Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information is an UNCLASSIFIED publication issued by the **Canadian Centre for Cyber Security** that guarantees the data authenticity, confidentiality and integrity, authentication and accountability, and non-repudiation where several algorithms may be required to satisfy these security requirements. Each algorithm should be selected and implemented to ensure these requirements are met.

This Canadian document provides a minimum set of requirements that a server must implement to meet these guidelines. Requirements are organized in the following sections:

- TLS protocol version support
- Server keys and certificates
- Cryptographic support
- TLS extension support
- Client authentication
- Session resumption
- Compression methods
- Operational considerations

Specific requirements are stated as either implementation requirements or configuration requirements. Implementation requirements indicate that federal agencies shall only procure TLS server implementations if they include the required functionality or can be augmented with additional commercial products to meet the needs. Configuration requirements indicate that TLS server administrators are required to verify that particular features are enabled or disabled, or in some cases, configured appropriately, if present.

Since this system keeps evolving and changes daily, the best option is to read the document directly from the source, from the link below.

Review [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information - ITSP.40.111]

✓ Mark Completed

← Previous
Cryptography Recap

Next →
Common Encryption Methods Quiz

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W07D2

Tue Aug 6

› Outline & Notes (1)

› Lectures (1)

⌄ Work (6)

5 hrs

- Case Studies: Encyption & Data Breach
- Cryptography Recap
- Cryptographics Algorithms
- ? Common Encryption Methods Quiz
- Differences Between SSL and TLS
- </> Unpacking Linux Commands Using AI Tools

W07D2 Schedule »