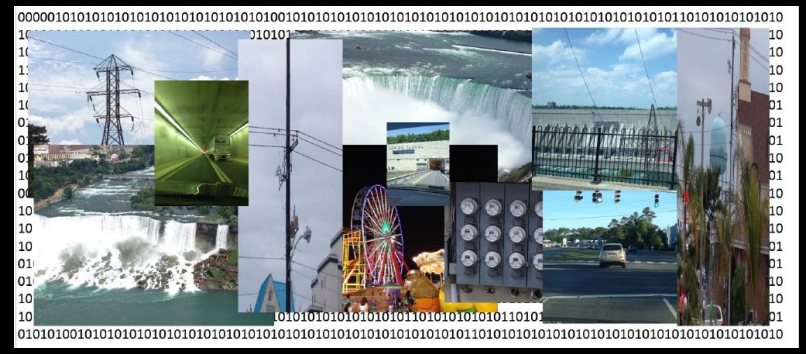
Advanced Cryptography Concepts



Dr. Dwayne Hodges, USA, (Ret.)

CISSP, CCISO, CEH, CNDA, ECES, SEC+
ITIL

Advanced Cryptography Concepts

Goals of Cryptography

Confidentiality

Integrity

Availability

Non-Repudiation

Advanced Cryptography Concepts

Applicable Standards and Agencies

Advanced Cryptography Concepts

National Institute for Standard Technology (NIST) Responsible for developing cryptographic standards and guidelines for non-national security systems for the Federal Government

National Security Agency (NSA)- The NSA has lots classified algorithms, participates in standards and works closely with other agencies such as NIST and categorizes encryption into four types and two suites.

Federal Information Processing Standards (FIPS) Standards that describe encryption algorithms and other information technology standards for use within non-military government agencies.

Public Key Cryptography Standards (PKCS) A group of public key cryptography standards developed and published by RSA.

Request for Comment (RFC)- Publications from the Internet Engineering Task Force (IETF), the principal technical development and standards setting bodies for the Internet. RFCs generally informational or experimental in nature and are not standards.

Committee on National Security Systems Provides guidance for security standards for federal agencies on national security systems.

Advanced Cryptography Concepts

National Institute for Standard Technology (NIST) Special Publications (SP)

- **SP 800-32 Introduction for Public Key Technology and the Federal PKI Infrastructure**
  - PKI functions, Security Services, PKI Infrastructure, Federal PKI, Polices and Procedures
- **SP 800-57 Part 1 Recommendation for Key Management**
  - Provides general key-management guidance for developers and system administrators
- **SP 800-57 Part 2 Recommendation for Key**
- **Management**
  - System or application owners, identifies appropriate key-management infrastructures, establishes organizational key-management policies, practices and plans.
- **SP 800-57 Part 3 Recommendation for Key Management**
  - Addresses key management issues with cryptographic mechanisms, provides guidance to system installers, system administrators, purchasers of PKI systems
  - *List goes on -*

Advanced Cryptography Concepts

Federal Information Processing Standards (FIPS)

- FIPS 180-2: Secure Hash Algorithm (SHA-1)
- FIPS 186: Digital Signatures
- FIPS 197: AES
- FIPS 198: Hash-based Message Authentication Code (HMAC)
- FIPS 140-3 Recommendations for Key Management

Advanced Cryptography Concepts

Public Key Cryptography Standards (PKCS)

PKCS #1- RSA *Cryptography Standard- provided standards for RSA*

PKCS

PKCS # 3 DH- Key Agreement Protocol

PKCS PKCS # 5 Password Based Encryption standard

PKCS # 6 Extended Certificate Syntax Standard

PKCS

PKCS

PKCS # 9 PKCS DS

PKCS # 10 Certificate Request

PKCS

PKCS

PKCS # 13 ECC

PKCS # 14 PRNG

PKCS

Advanced Cryptography Concepts

Request for Comment (RFC)- publications from the (IETF) that are informational purposes and are not standards are generally standards are “born” from them

Advanced Cryptography Concepts

Request for Comment (RFC)- examples

RFC 8221- Cryptographic Algorithm Implementation Requirements and Usage Guidance

- For Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 1704- Authentication requirements of computing systems and network protocols

Advanced Cryptography Concepts

Committee on National Security Systems

- CNSSI 1300 Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25
  - Provides guidance for security for TS intelligence PKI community

Advanced Cryptography Concepts

NSA is the de facto Standard

Suite A

- Not Published
- Classified
- Contains algorithms that will not be release
- Used to encrypt especially sensitive information , ECDSA, ECDH, SHA-256, SHA-384)

Suite B

- Published
- Included AES with key size of 128 and 256

Advanced Cryptography Concepts

4 Types

1. Type 1

   Used for classified or sensitive government information, to include crypto equipment

   NSA certified Type 1 products include:

   - Junifier- Block Ciphers
   - MAYFLY Asymmetric
   - Walburn, High Band Link Encryption
   - FASTHASH, Hashing
   - PEGAGUS, Satellite Telemetry

2. Type 2

   Used for unclassified cryptographic equipment *endorsed* by NSA

   SkipJack

   KEA

3. Type 3

   (SBU), excluding National Security Systems

   - AES, 3DES, SHA

4. Type 4

   Algorithms that are registered by NIST, but are NOT published by FIPS

Advanced Cryptography Concepts

“The strength in cryptographic systems comes by following standards”