



Cryptography

An InfoDefense Training Course
CISSP Domain Session 04

Christopher Davis
davischr2@gmail.com
www.linkedin.com/in/christopherdavis

Overview

- The professional should fully understand:
 - Definitions
 - History
 - Cryptography Fundamentals
 - Symmetric Key Cryptosystem Fundamentals
 - Asymmetric Key Cryptosystem Fundamentals
 - Digests
 - Cryptographic Attacks
 - Public Key Infrastructure Concepts
 - Key Distribution and Management Issues





Crypto History

- Kryptos Graphein – "Secret Writing" - Cryptography
- 2-3000 B.C. Hieroglyphics
 - Egyptian scribes uses non-standard hieroglyphics in inscriptions
 - First known documented example
- 400 B.C. Spartans – Scytale
 - Strip of papyrus or parchment wrapped around a wooden rod
- 800 A.D. Arabs – Cracking the Code – Cryptanalysis
- Jefferson Disks
- Japanese Purple Machine
- German Enigma Machine

TELEGRAM RECEIVED.

MAILED
October 1-8-58
V. ...son, State Dept.

By *Max A. Eckhoff*
Date *Oct 27, 1958*

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, ~~invite~~ ^{invite} Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMAN.

Example of Encrypted Volume

- 256-Bit BlowFish Encrypted Volume:

```
||Î ||iDu-iYô%IA *hB 7|šH ²»||iö CG G òÁæE3z)||P|^Éyé2v FAä||iy
Ōú-b ||c|WDD`ONĐØ| æutÁ3N, gC |y||Njw&³[ç\k oóUíøª| bòa||iO@úÜOLá|
||!tô.Á|{()E Èztš@f~ú _'È~cúgi áy{Tè|žòjá|²w È>N»Ö ||P²||7KÆ¹ÉJ|
CÁ -|šBiRa||ži |4Ū| 7µ SZ*:|>|ççš||šx|i~ |ēB ü `²ž|?~ær@Đó'»*Ōáú
àá G }Lz|xDēø|XtŸJ!-|»U|) ||÷Ū úÁ'ý8Ū||{š|š. %|ápóÄAnábšÉ|| ± È
<|Qpš6:,|³ qžŌÁ||N¹¹4imèAXýp³3|éNú x '|paS÷ |WŌ%rYk || VŌ4E &%
% 41|-HÓU~ 'ÉTr8i²y pM $ žD :`cùFb-`uyâ áfŇ:Ī< DÆi á||VšoÄeÄ-1É
@11~9ÄšÜŌ?{~||#Ÿ|F 6S<'DPš7ÉTaĐSžNT 8AC|xÆaNšDkxVž÷GŪĪT'1|A %š
ú|||a%| Á3|š@] ÷- |ü\|-8@ç|É||?r | ||cŌ~zše|H'z ŪR ||:QÉ~ | f4á
Ä|L|:( iävM¹x@{tájE #ÍÁè| [&Ň|R ||Ūp|Le -ýŌ|B5x-ŪJáÄè| XH|} Ō á
V .úKÄ|òpçwwÉGXŪ¹Á|ü| 2== Nq YÈ Tā#|òÁiò³| Wd'šfv ýÉcz~jæ|ö:cĪ7
BÄXOiyá@ÁLPá š|||Áfçü|üI9(|+4ÂN&È EVúÁa|kŸ%+|šD @N|á' ||DPŌtDšJB|
óÁjĪ¹Īi *¹Ī m~ øNi'žPç. o|2|~@toŪ| WáĪ²-i óc²`ááú ²ĐTHB éª|EŌš
```



Definitions

Definitions

- Plain Text
- Ciphertext or Cryptogram
- Cryptanalysis
- Cryptographic Algorithm – Cipher
- Decipher – Decode – Decrypt
- Encipher – Encode – Encrypt
- Key or Crypto variable
- Work Function (or Work Factor)



Cryptography Fundamentals

Concept 01: Method and Key

- Method
 - Tumbler mechanism
 - Physical lock or machine
 - Algorithm
- Key
 - Combination; physical key
 - Work factor: amount of time to try all possible combinations or keys before breaking the lock
 - Algorithms should support many keys

Concept 02: Block and Stream

- Block
 - Fixed chunks are encrypted
 - Results in the same length output
 - Example: 64bit chunks of data
 - You'll do this exercise later

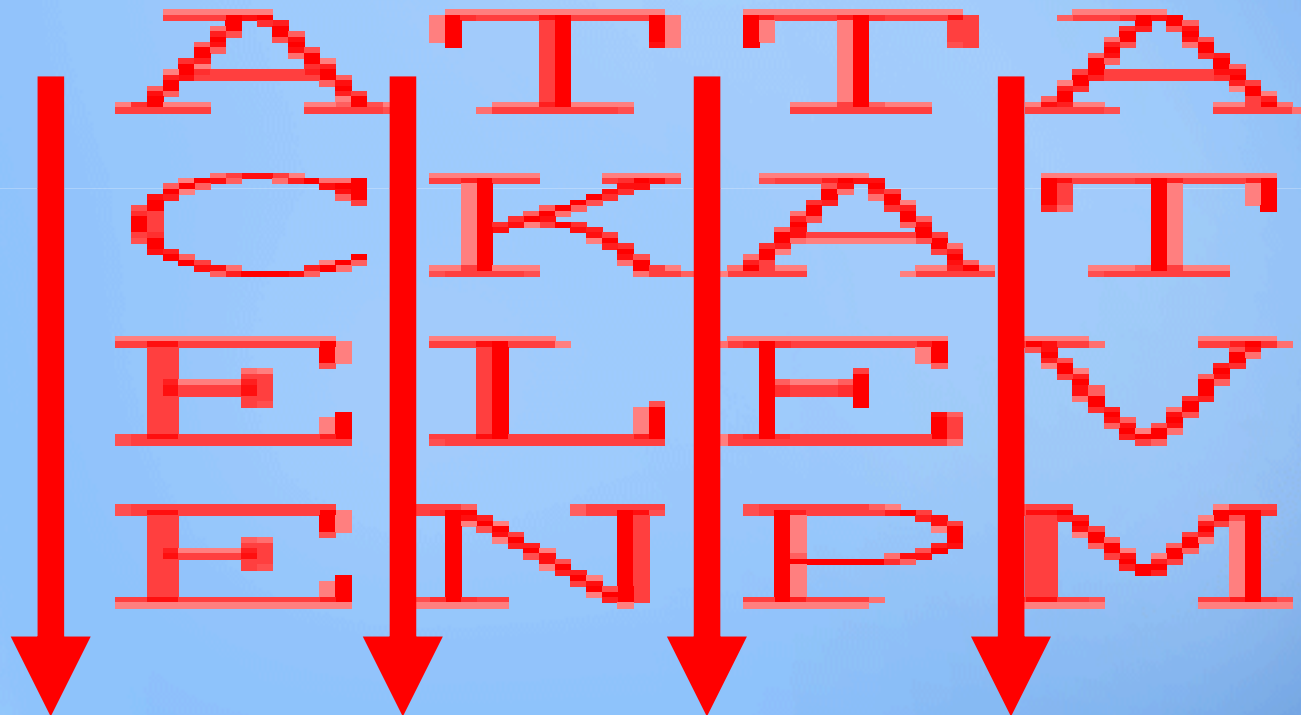
- Stream
 - Generates a key stream
 - Combines keystream with plaintext
 - Usually XOR operation

Crypto Fundamentals

- Classic Ciphers
 - Substitution
 - Replaces each letter of the plaintext with another that is farther down the alphabet
 - Caesar “C3” Cipher
 - Transposition (or “Permutation”)
 - Keeps but shifts plaintext letters
 - Can get complicated
 - Grids: Length and Width
 - Cracked using frequency analysis
 - Strengthened when coupled with Substitution and placed in multiple rounds of encoding
 - Polyalphabetic Cipher
 - The Book... or Running Key Cipher (e.g. using Bible)
 - Codes (e.g. Submarine Battle Stations Missile)
 - Steganography – Steganos Graphein (Covered Writing)

Transposition (Permutation) Example

ACEETKLNTAEPATVM





Cryptography Attacks

Yeah – It's Your Birthday

The Birthday Paradox

- What's the size of the group with a 50% probability that:
 - Someone shares the same birthday as YOU?
 - Any two people share the same birthday?

Cryptographic Attacks: TYPES

The names come from the type of information available to the attacker:

- Ciphertext-only: Have cipher text only – attempting to **recover plaintext**
- Known-plaintext: Have cipher and plain text – attempting to **recover key**
- Chosen-plaintext: e.g. **have the engine**
- Adaptive-chosen-plaintext
- Chosen-ciphertext: e.g. trial decryption – **verify your understanding**
- Adaptive-chosen-ciphertext:

Cryptographic Attacks: METHODS I

- Brute-Force: Exhaustive search
 - Permutations
 - Rainbow tables
- Symmetric Block Cipher Attacks:
 - Differential Cryptanalysis
 - Chosen plaintext attack
 - Probabilities are assigned to keys
 - Linear Cryptanalysis
 - Known plaintext attack
 - Acts on pairs to create information about the keys
 - Weak Keys
 - E.g. DES – 4 keys that are same as encrypt and decrypt
 - Usually filtered
 - Algebraic Attacks
 - Rely on block ciphers having lots of structure
 - Some special cases encrypting twice with same key doesn't offer any more security

Cryptographic Attacks: METHODS II

- Stream Cipher Attacks
 - Analyzing the Initialization Vector used in the generation of the key stream
 - Key stream is used to encrypt data
- Man in the Middle
 - Think “I’ll proxy that handshake for you – thanks!”
- HASH Attacks test whether hashes are
 - One-way functions
 - Collision free (different sources – same output)

PART II: CRYPTOSYSTEM FUNDAMENTALS

Symmetric
Asymmetric
Digest



RED



RED



Symmetric Key Cryptosystem Fundamentals

Symmetric Key Cryptography

- “Secret Key” or “Shared Key”
- This crypto-system uses the same key for both encryption and decryption
- Both the sender and the receiver need to have the same key in order to communicate successfully
- Formula for number of keys needed for secret communications among users:
 - ‘n’ = # people involved
- Examples: DES, 3-DES, RC4, RC5
- How it works

$$\frac{n(n-1)}{2}$$

Symmetric Key Pros & Cons

Advantages

- 1000 times faster than public key cryptography;
- Considered secure, provided the key is relatively strong
- The ciphertext is compact (that is, encryption does not add much excess “baggage” to the ciphertext);
- Widely used and very popular.

Disadvantages

- The administration of the keys can become extremely complicated;
- A large number of keys is needed to communicate securely with a large group of people;
- Non-repudiation is not possible (see sidebar for a detailed discussion on nonrepudiation);
- The key is subject to interception by hackers.

Symmetric Ciphers

- DES
 - Usually implemented in software:
 - Electronic Code Block (ECB) (Block cipher)
 - Cipher Block Chaining (CBC) (Block cipher)
 - Usually implemented in hardware:
 - Cipher Feedback Mode (CFB) (Stream cipher)
 - Output Feedback (OFB) (Stream cipher)
- Triple DES – more secure than DES
- Rijndael Block Cipher (AES-128, 192 or 256)
 - Advanced Encryption Standard
- Twofish Algorithm
- IDEA Cipher
- RC5



GREEN



RED



Asymmetric Key Cryptosystem Fundamentals

Asymmetric Key Cryptosystems

- “Public Key”
- This crypto-system uses one key for encryption and another key for decryption
- Each user has two keys – one **public** key, which is revealed to all users, and one **private** key, which remains a secret. The private key and the public key are mathematically linked;
- Encryption is performed with the public key and decryption is performed with the private key;
- Examples: RSA, Elliptic Curve Cryptography (ECC).

Asymmetric Pros & Cons

Advantages:

- Considered very secure;
- No form of secret sharing is required, thus reducing key administration to a minimum;
- Supports non-repudiation, confidentiality, access control, authentication, data integrity (with hash)
- The number of keys managed by each user is much less compared to secret key cryptography.

Disadvantages:

- Much slower compared to secret key cryptography;
- The ciphertext is much larger than the plaintext, relative to secret key cryptography.

Asymmetric Key Algorithms

- Diffie-Hellman Key Exchange
 - Used for KEY EXCHANGE
 - Also called exponential key agreement
- El Gamal
 - Extension of Diffie-Hellman – approaches RSA such that it allows for message encryption
 - Works using discrete logs
- Merkle Hellman Knapsack
 - Very complicated math – e.g. “number of objects with given weights from a large set such that the sum of the weights is equal to a pre-specified weight..”
- Elliptic Curve (EC)
 - For the curious: $y^2 + y = x^3 * x^2$



Message Digests

Message Digests

- Designed specifically to guarantee message integrity
- Message digests achieve data integrity by applying complex math to data to ensure that this data has not been tampered with on route to its final destination.
- Message digests take in a variable length input and generate a fixed length output called the “hash” or a message digest
 - MD5 algorithm generates a 128-bit digest
 - SHA-1 algorithm generates a 160-bit digest);
- It is not computationally feasible to calculate the message based on the digest;
- It is not computationally feasible to find two messages which will generate the same digest (this feature is also called “collision resistance”).



Thank You

Chris Davis, CISSP, CISA
davischr2@gmail.com