

**“Too Many Secrets”  
Cryptography 101**


Chris Hare, CISSP, CISA  
Information Security Advisor  
Nortel Networks  
Security Engineering



**What you don't know will  
keep you safe**

**HOT!**


(C) 2002 Chris Hare. All Rights Reserved



## Too Many Secrets

- ◆ Cryptography Defined
- ◆ Terminology
- ◆ History
- ◆ Why Cryptography?
- ◆ How it Works
- ◆ Basics
- ◆ References


(C) 2002 Chris Hare. All Rights Reserved



## What is Cryptography?

- ◆ The Art of finding new ways to hide messages
- ◆ Codes.... But not just any code. Unbreakable code.


(C) 2002 Chris Hare. All Rights Reserved



## The Basics - Terminology

- ◆ **Plaintext** – the original, readable message
- ◆ **Encryption** – the process of scrambling or hiding the plaintext
- ◆ **Ciphertext** – the scrambled message
- ◆ **Decryption** – the process of descrambling the ciphertext to reveal the message
- ◆ **Cryptography** – finding ways to encrypt messages
- ◆ **Cryptanalysis** – finding ways to defeat cryptographic algorithms

(C) 2002 Chris Hare. All Rights Reserved



## A Little History

- ◆ Hebrew scribes used the ATBASH cipher to write the book of Jeremiah. (500-600 BC)
- ◆ **Julius Caesar** used a simple substitution cipher (50-60 BC)
- ◆ **Blaise de Vigenère** wrote a book on ciphers. (1585)
- ◆ The Enigma machine became the cryptographic workhorse of Nazi Germany. (1933-1945)
- ◆ The Japanese Purple machine was invented. (1937)
- ◆ IBM develops the U.S. Data Encryption Standard. (1976)
- ◆ **Whitfield Diffie** and **Martin Hellman** introduce the idea of public key cryptography. (1976)
- ◆ **Ronald L. Rivest**, **Adi Shamir** and **Leonard M. Adleman** develop a practical public-key cipher. (1977)
- ◆ **Phil Zimmermann** released his first version of PGP (Pretty Good Privacy). (1991)
- ◆ The Rijndael algorithm is selected as the new U.S. Advanced Encryption Standard to replace DES. (2001)


(C) 2002 Chris Hare. All Rights Reserved



## Why Cryptography

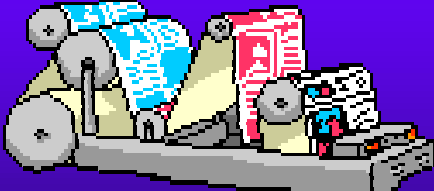
- ◆ Identification & Authentication
- ◆ Secure Communications
- ◆ Electronic Commerce
- ◆ Remote Access
- ◆ Wireless
- ◆ Other applications

(C) 2002 Chris Hare. All Rights Reserved



## How it Works

apel348gsb  
m9jrht20qw



**Key** **Plain Message**

(C) 2002 Chris Hare. All Rights Reserved



## Mirror, Mirror ...

- ◆ Symmetric

- Uses one “shared secret” key



- ◆ Asymmetric

- Uses two keys
- One to encrypt, one to decrypt




(C) 2002 Chris Hare. All Rights Reserved



## Keys...

- ◆ Encryption requires an algorithm and a key
- ◆ The **algorithm** describes **how** the data is encrypted
- ◆ The **key** provides the **variable** affecting the operation of the algorithm


(C) 2002 Chris Hare. All Rights Reserved



## And more Keys

- ◆ The strength of the algorithm is affected by the key
- ◆ Shared secret keys are known by those who must exchange information
- ◆ Public Key Cryptography uses
  - A Public key available to anyone
  - A Private key known only to the owner


(C) 2002 Chris Hare. All Rights Reserved



## Cipher Types

- ◆ Substitution
  - Caesar
  - ROT-13
  - Polyalphabetic
- ◆ Transposition
  - Columnar
- ◆ Streaming
  - One Time Pad
- ◆ Block


(C) 2002 Chris Hare. All Rights Reserved



## Substitution

- ◆ Replacing one character or symbol with another
- ◆ Simple and easily defeated
- ◆ Most common is the Caesar Cipher
  - Shift three characters right for encryption
  - Shift three characters left for decryption
- ◆ ROT-13 shifts right by 13 characters for both encryption and decryption
  - All users know or have the key

(C) 2002 Chris Hare. All Rights Reserved




## The Caesar Cipher

**A T T A C K   A T   D A W N**

Command	Explanation
\$ cat z attack at dawn	Display the file "z"
\$ ./caesar.pl --encrypt z dwwdfn dw gdzq	Encrypt using Caesar cipher Encrypted message
\$ ./subst.pl --decrypt --key 5 a _rr_ai_r b_ul	Decrypt using wrong "key" Undecipherable message
\$ ./subst.pl --decrypt --key 3 a attack at dawn	Decrypt using correct key Plain text message


(C) 2002 Chris Hare. All Rights Reserved



## ROT-13

\$ cat z	Show the file z
attack at dawn	
\$ ./rot13.pl --encrypt z	Encrypt file z
nggnpx ng qnja	Encrypted message
\$ ./rot13.pl --decrypt z	Decrypt the file z
nggnpx ng qnja	Same encryption
\$ ./rot13.pl --encrypt z > a	Encrypt file a
\$ ./rot13.pl --decrypt a	Decrypt file a
attack at dawn	Actual message

(C) 2002 Chris Hare. All Rights Reserved



## Transposition

- ◆ Doesn't alter the characters
- ◆ Transposes or re-arranges them
- ◆ Different forms
  - Simple Transposition
  - Split to 5 character groups
  - Columnar

(C) 2002 Chris Hare. All Rights Reserved



## “Setec Astronomy” Simple Transposition

S E T E C  
A S T R O N O M Y


(C) 2002 Chris Hare. All Rights Reserved



## 5 Character Grouping

- ◆ Split into groups  
Everything is coming up roses  
Every|thing|is co|ming | up r|oses
- ◆ Apply key to rearrange the letters  
Eyver tghim ios c m ing rup o ses
- ◆ Not very strong
- ◆ Subject to frequency analysis


(C) 2002 Chris Hare. All Rights Reserved



## Combination

- ◆ Use multiple substitution and transposition
- ◆ High degree of abstraction
- ◆ Frequency analysis and other attacks more difficult


(C) 2002 Chris Hare. All Rights Reserved



## Streaming Ciphers

- ◆ Process “streams” of data
- ◆ One Time Pad
  - Plain Message + Single Use Key = Cipher
- ◆ Both sender and receiver must have the same “pad”
- ◆ Example of theoretically unbreakable cipher
  - By brute force
  - Pad could be stolen or lost
  - Pad cannot be re-used


(C) 2002 Chris Hare. All Rights Reserved



## Block Ciphers

- ◆ Can operate in both symmetric or asymmetric depending upon implementation
- ◆ Example block ciphers:
  - Advanced Encryption Standard (Rijndael)
  - Data Encryption Standard
    - Triple DES
  - CAST
  - Blowfish
  - IDEA
  - RC2, RC5
  - Skipjack
  - Twofish


(C) 2002 Chris Hare. All Rights Reserved



## Block Modes - ECB

- ◆ Electronic Code Book (ECB)
  - Same plaintext produces the same ciphertext
  - Common phrases can be encoded into a “codebook”
  - Allows retrieval of the message without the key
  - Allows for random data access without having to decrypt entire files


(C) 2002 Chris Hare. All Rights Reserved



## Block Modes – CFB & OFB

- ◆ Cipher Feedback (CFB)
  - Implemented as a stream cipher
  - Processes data less than or equal to the block size of the cipher
  - Can resynchronize after data loss
  - Military Ciphertext Auto Key (CTAK)
- ◆ Output Feedback (OFB)
  - Works like CFB
  - Principle difference is key generation

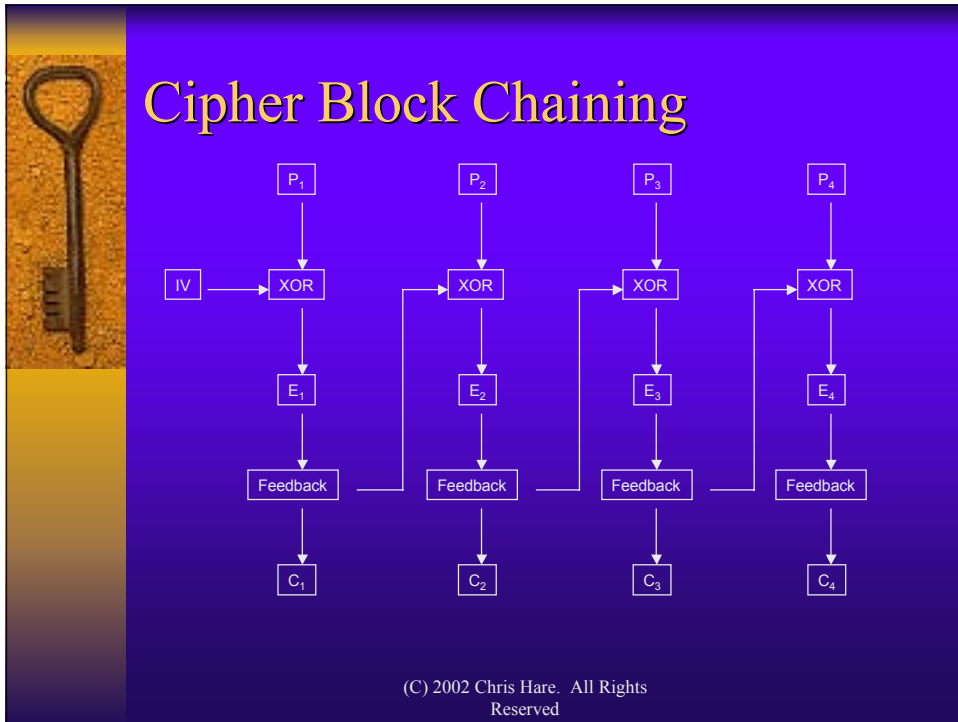
(C) 2002 Chris Hare. All Rights Reserved




## Block Modes - CBC

- ◆ Cipher Block Chaining (CBC)
  - Overcomes the ECB problem
  - Uses output of the previously encrypted block to encrypt the next block of data
  - Uses an Initialization Vector (IV) to initialize the encryption process
  - The IV can be transmitted with the ciphertext

(C) 2002 Chris Hare. All Rights Reserved




- 
- ## Cryptanalysis
- ◆ Methods used to obtain a key (possibly algorithm) from the plaintext, ciphertext or both
  - ◆ Differential
    - Compares specific  $c$  pieces of ciphertext to determine the key
    - Uses plaintext with specific differences
    - Comparison of ciphertext yields key possibilities
  - ◆ Linear
    - Generic analysis method
    - Dependent upon probability of relationship between the plaintext and the key
- (C) 2002 Chris Hare. All Rights Reserved



## Related Key

- ◆ Dependent upon weaknesses in the cipher
- ◆ Two closely related keys may yield enough information to obtain the real key
- ◆ Most modern ciphers are resistant to related key attacks


(C) 2002 Chris Hare. All Rights Reserved



## Cryptographic Attacks

- ◆ Ciphertext Only Attack
  - Uses several examples of ciphertext
  - Cryptanalyst may know the algorithm
- ◆ Known Plaintext Attack
  - Cryptanalyst has plain and cipher text
  - May know the algorithm
- ◆ Chosen Plaintext Attack
  - Cryptanalyst can choose the plaintext
  - Has encryption engine, but algorithm is unknown
  - Can analyze resulting ciphertext
  - Attempting to deduce key for future messages


(C) 2002 Chris Hare. All Rights Reserved



## Cryptographic Attacks

- ◆ Adaptive Chosen Plaintext Attack
  - Same as Chosen Plaintext, but cryptanalyst can adjust plain text
- ◆ Chosen Ciphertext Attack
  - Cryptanalyst chooses the ciphertext to decrypt
  - Has access to resulting plain text
  - Commonly used against asymmetric systems

(C) 2002 Chris Hare. All Rights Reserved



## Cryptographic Attacks

- ◆ Brute Force Attack
  - Trying every possible key
- ◆ “Purchase key” Attack
  - One of the simpler attacks – buy the key through bribery, extortion or blackmail
- ◆ “Rubber Hose” Attack
  - “Beat it out of them!”

(C) 2002 Chris Hare. All Rights Reserved




## The Dangers are Clear

- ◆ Applying cryptographic techniques can protect
  - Financial Institutions and the economy
  - Power and Utilities
  - Communications
  - Air Traffic Control
  - Military applications

The loss of cryptographic keys exposes any or all of these systems to threat and attack


(C) 2002 Chris Hare. All Rights Reserved



## Summary

- ◆ Brief introduction to cryptography basics
- ◆ Selection of appropriate implementation
  - Type of information and application


(C) 2002 Chris Hare. All Rights Reserved



## References

- ◆ Applied Cryptography. Bruce Schneier
- ◆ Cryptography Decrypted. Doris Baker, H. X. Mel
- ◆ RSA Security's Official Guide to Cryptography. Steve Burnett, Stephen Paine
- ◆ Cryptography 101. Chris Hare (Auerbach)
- ◆ Many references online.

(C) 2002 Chris Hare. All Rights Reserved



## Questions?

Chris Hare, CISSP, CISA  
[CHare@NortelNetworks.com](mailto:CHare@NortelNetworks.com)

(C) 2002 Chris Hare. All Rights Reserved