James P. Cavanagh

Global Telecom & Security Consultant

Presents

Introduction to Encryption

An Online Briefing for Webtorials
December 2001

www.consultant-registry.com

www.webtorials.com

 jcavanagh@consultant-registry.com

Presenter

James P. Cavanagh

Global Telecommunications Consultant

jcavanagh@consultant-registry.com

www.consultant-registry.com

 jcavanagh@consultant-registry.com

Outline

Introduction to Encryption

- Why is this Important?
- Encryption Definition
- Cryptography vs Encryption
- Applications
- Playfair Cypher Example
- DES Example
- 3DES Example
- AES, PGP, SSL, IPSEC and PKI
- Encryption Issues and Myths
- Encryption and Business
- Conclusion

 jcavanagh@consultant-registry.com

Why is this important?

Introduction to Encryption

While encryption has been used in some form since ancient times it has become important more recently for a variety of applications from protecting corporate and government secrets and financial transactions to use by hackers, terrorists, pornographers and industrial spies to hide their illegal activities.

It is the wide variety of applications that make encryption such a "hot topic" in both the technical and non-technical realms.

 jcavanagh@consultant-registry.com

Introduction to Encryption

Encryption is a systematic means of scrambling information such that it is unintelligible in its encrypted form but may be unscrambled by an intended recipient revealing the original message.

Encryption uses a shared "key" or procedure to perform the scrambling and unscrambling. The specific encryption process may be known, but a message may still be kept secret.

 jcavanagh@consultant-registry.com

Introduction to Encryption

The three objectives of encryption are:

(1) Assuring privacy/confidentiality of information during transmission.

(2) Assure that messages and digital signatures have not been tampered with.

(3) Verifying the authenticity of the source of the message*.

*** While this is an objective of encryption, this is only possible with private key cryptography, where a secret key is shared between the parties. Public key encryption does not, automatically, provide authenticity because the key used for encryption is publicly available. More on this later.**

 jcavanagh@consultant-registry.com

Cryptography vs Encryption

Introduction to Encryption

Cryptography comes from the Greek:

κρνπτο ✚ γραφη

Hidden or Secret + Writing

"**Cryptography** *is the art of secret writing, and* **encryption** *is the process of making the writing secret."*

 jcavanagh@consultant-registry.com

Applications

Introduction to Encryption

- **Information Privacy / Confidentiality**
  - **During Transmission**
  - **While Stored**
  - **Used for Centuries**
    - **Keep Industrial Processes Secret**
    - **Hide Religious Rites and Rituals**
    - **Maintain Privacy of Diplomatic and Personal Correspondence**
- **Source Authentication**
  - **Assure Source is Authentic**
  - **Avoid Message Modification**
  - **Avoid Message Substitution**

 jcavanagh@consultant-registry.com

Introduction to Encryption

Playfair Cypher

What is it?

- Encryption Methodology / Also Authentication
- Developed for Telegraph Secrecy
- Used in Boer War, WWI, WWII and Australian Coastal Security
- Developed in 1854 by Sir Charles Wheatstone
- Named after Lyon Playfair
- Used by John F. Kennedy after sinking of PT-109 to call for Help

Why do we care?

- Further Advancement in Cryptography
- More Sophisticated
- More Difficult to Crack
- Simple to Encode / Decode
- Use of "Soft" Key - More Flexible

Sir Charles Wheatstone

 jcavanagh@consultant-registry.com

Playfair Cypher Example

Introduction to Encryption

Playfair Cypher

Keyword: DILBERT
Plain Text: PICADILLY CIRCUS

How does it work: Playfair Encryption

1 Choose a Keyword without repeating letters
2 Write the Keyword in the Matrix
It may be written in any manner as long as sender and receiver are consistent
3 Fill in the remaining Alphabetic Letters. I and J are combined.
4 Prepare the Plain Text for Encryption:
Break it up into two-letter groups
If both letters in a pair are the same, insert an X between them.
If there is only one letter in the last group, add an X to it.

D	I	L	B	E
R	T	A	C	F
G	H	K	M	N
O	P	Q	S	U
V	W	X	Y	Z

5 x 5

Plain Text Ready for Encryption: PI CA DI LX LY CI RC US

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

Playfair Cypher Example

Introduction to Encryption

Playfair Cypher

How does it work: Encryption

(continued)

5 Now we Encrypt the Pairs of Letters
6 Find the Rectangle made by P and I in the matrix. P and I are in the SAME COLUMN and don't form a rectangle. Use the letters below. This would be WT.
7 Now encrypt CA. They are in the SAME ROW, so use the letters to right. Therefore: FC.
8 Now encrypt DI. This is IL.
9 Encrypt LX. This is AL

D	I	L	B	E
R	T	A	C	F
G	H	K	M	N
O	P	Q	S	U
V	W	X	Y	Z

Plain Text Ready for Encryption:
PI CA DI LX LY CI RC US

Encrypted Message: WT FC IL AL

 jcavanagh@consultant-registry.com

Playfair Cypher Example

Introduction to Encryption

Playfair Cypher

How does it work: Encryption

(continued)

10 Encrypt LY. This forms a rectangle. Take the letter pair formed in opposite corners of the rectangle, starting with the letter on the row of the first letter. This would be: BX.
11 Now encrypt CI. The result is TB.
12 Now encrypt RC. The result is TF.
13 Now encrypt US. The result is VU

D	I	L	B	E
R	T	A	C	F
G	H	K	M	N
O	P	Q	S	U
V	W	X	Y	Z

Plain Text Ready for Encryption:
PI CA DI LX LY CI RC US

Encrypted Message: WT FC IL AL BX TB TF VU

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

Playfair Cypher Example

Introduction to Encryption

Playfair Cypher

How does it work: Decryption

1 Reverse the process.
2 If two characters are on the same row take the characters to the left.
3 If two characters are on the same column take the characters above
4 If the letters make a rectangle, take the letters in opposite corners, taking the first letter first, then the second of the pair.
5 Now decrypt this message:
WT FC IL AL BX TB TF VU

D	I	L	B	E
R	T	A	C	F
G	H	K	M	N
O	P	Q	S	U
V	W	X	Y	Z

Decrypted Message:

PI CA DI LX LY CI RC US

 jcavanagh@consultant-registry.com

Playfair Cypher Example

Introduction to Encryption

Playfair Cypher

Keyword: WEBTORIALS

How does it work: Decryption

1 Reverse the process.
2 If two characters are on the same row take the characters to the left.
3 If two characters are on the same column take the characters above
4 If the letters make a rectangle, take the letters in opposite corners, taking the first letter first, then the second of the pair.
5 Now decrypt the following message. Don't worry, this message will appear again on the final screen so that you will have time to write it down.

LRWDJWEPOJRLDTACEQAVDVFRXIFXHCFXHJOBEJBLTGSW

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

Playfair Cypher Example

Introduction to Encryption

Playfair Cypher

Pros	Cons
Simple, Easy, Automated Does Not Require Code Book Uses Same Character Set for Everything Difficult to Crack	Exchange of Keyword must be secure

 jcavanagh@consultant-registry.com

DES Example

Introduction to Encryption

Data Encryption Standard (DES)

What is it?
- A US Government Encryption Algorithm
- Based on the IBM Lucifer Cipher with NSA "input"

Why do we care?
- Fast, safe, reliable (by 1976 standards)
- Basis of many, many other algorithms and products including subsequent 'flavors' of DES
- Historically hardware based

 jcavanagh@consultant-registry.com

Introduction to Encryption
Data Encryption Standard (DES)

How does it work?

1 Input is 56 bit key and 64 bit Plain Text"

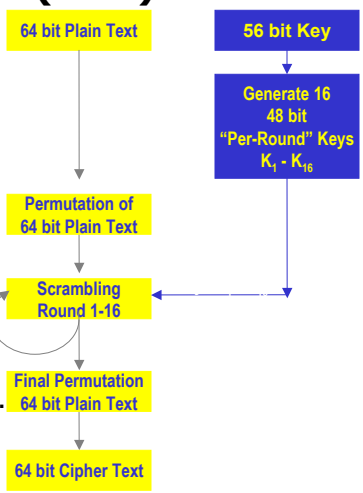
2 Generate 16 keys 48 bits in length for each of 16 rounds of scrambling

3 Perform "Initial Permutation" of Data Matrix. This makes DES more difficult to implement in software, but does not enhance security.

4 Sixteen rounds of scrambling now occur, each using a different one of the per-round keys.

5 Final Permutation now rearranges the matrix.

6. DES Encrypted Cipher Text



 jcavanagh@consultant-registry.com

Introduction to Encryption
Data Encryption Standard (DES)

Pros	Cons
Simple, safe, secure (by 1970s standards), but today not considered to be secure enough for many applications Around since mid 1970s Parity Checking on Key	56 bit key length (64 bit key space - 8 bits for parity) Barely considered secure in 1977 Not considered secure today Possibly weakened to allow cracking by NSA Historically not legal for export

 jcavanagh@consultant-registry.com

Introduction to Encryption
Triple DES (3DES)

What is it?
- A US Government Encryption Algorithm
- Based on DES
- DES is considered “broken”, 3DES is the “fix”
- “168 bit” Key is actually 3x56 Bit Keys

Why do we care?
- Widely used in commercial applications
- Dramatically decreases likelihood of Brute Force Attack
- Cryptographically much stronger than DES
- Approved for Export
- It is believed that NSA Computers can crack 3DES

 jcavanagh@consultant-registry.com

3DES Example

Introduction to Encryption
Triple DES (3DES)

How does it work?

1 Input is 168 bit key and 64 bit Plain Text

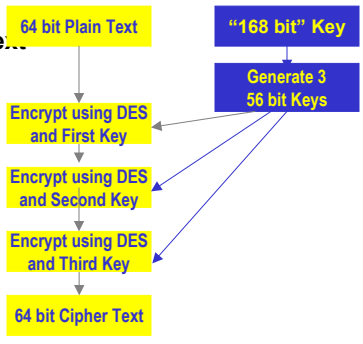
2 Generate 3 keys 56 bits in length

3 Encrypt Using First Key and DES

4 Encrypt Using Second Key and DES*

5 Encrypt Using Third Key and DES

6 3DES Encrypted Cipher Text



** One commercial variation is to use Second Key to DECRYPT instead of ENCRYPT on this Step*

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

3DES Example

Introduction to Encryption

Triple DES (3DES)

Pros	Cons
Simple, safe, reasonably *secure* Around since mid 1970s Parity Checking on Key	56 bit key length three times - Not actually 168 bit key

 jcavanagh@consultant-registry.com

AES, PGP, SSL, IPSEC and PKI

Introduction to Encryption

Additional Standards and Protocols

- **Advanced Encryption Standard (AES)**
- **Pretty Good Privacy (PGP)**
- **Secure Sockets Layer (SSL)**
- **IP Security (IP Sec)**
- **Public Key Infrastructure (PKI)**

 jcavanagh@consultant-registry.com

Introduction to Encryption

AES

What is it?

- A New US Government Encryption Standard intended to replace DES by the end of 2001
- Based upon the Rijndael Algorithm
- Rijndael developed by Two Belgian Cryptographers

Why do we care?

- Replaces much weaker DES
- May or May Not (Likely Not) Important in non-Government eCommerce
- Many of us don't really care

 jcavanagh@consultant-registry.com

AES, PGP, SSL, IPSEC and PKI

Introduction to Encryption

Pretty Good Privacy (PGP)

What is it?

- "Public domain" encryption software
- Designed to protect eMail content
- Can be used to encrypt other types of messages
- Based on RSA

Why do we care?

- Released by Phillip Zimmermann of MIT as "guerrilla freeware" in 1991
- Distributed via Internet - *Globally*
- Subject to 3 year criminal investigation
- Challenged US Export Restrictions on Cryptography
- Defense : PGP is "artistic expression", covered under US Constitution as "freedom of expression"

"If privacy is outlawed, only outlaws will have privacy."
- Phil Zimmermann

 jcavanagh@consultant-registry.com

Introduction to Encryption

Secure Sockets Layer (SSL)

- Developed by Netscape
- Built Into Most Browsers
- Transport Layer Security (TLS) similar to SSL v3.0
- Enabled by Loading a Certificate
- Provides:
  - Data Encryption
  - Server Authentication
  - Message Integrity
  - Optional client authentication
- Three "strengths"
  - 40-bit DES
  - 128-Bit DES
  - 168-bit 3DES

 jcavanagh@consultant-registry.com

Introduction to Encryption

SSL Certificates

- Required on Server
  - Server Certifies its Identity to Client
- Optional on Client
  - Client Certifies its Identity to Server
- Issued by Certification Authority (CA)
  - Verisign / Thawte
  - General Electric
  - Entrust
  - Other

 jcavanagh@consultant-registry.com

Introduction to Encryption

IPSec

What is it?

- A "framework" for Internet Protocol Security
- Three Major Areas:
  - Authentication
  - Privacy / Encryption
  - Key Management
- Flexible but Complex
- Described in RFC2401

Why do we care?

- Security Framework (specifically) for the Internet, Intranets, Extranets and other IP-based networks
- Critical to Virtual Private Networks

 jcavanagh@consultant-registry.com

AES, PGP, SSL, IPSEC and PKI

Introduction to Encryption

IPSec

How does it work?

- Security of Three Relationships
- Two modes of operation
  - Transport Mode
  - Tunnel Mode
- Two Methods of Protecting Datagrams
  - Encapsulating Security Payload (ESP)
  - Authentication Header (AH)
- Two Implementations
  - Internal (Bump In The Stack (BITS))
  - External (Bump In The Wire (BITW))
- Internet Key Exchange (IKE)

© 2001 James P. Cavanagh, All Rights Reserved jcavanagh@consultant-registry.com

Introduction to Encryption

Public Key Infrastructure (PKI)

What is it?

- The "Trust" Structure for Public Key Applications
- Three Main Functional Components:
  - Certificate Authority (CA)
  - Repository for Keys, Certificates and Certificate Revocation Lists (CRLs)
    - Usually based on Lightweight Directory Access Protocol
  - Management Function (Typically GUI)

Why do we care?

- Widely used in commercial applications
- Basis for global eCommerce
- Cornerstone for IP VPNs

 jcavanagh@consultant-registry.com

Introduction to Encryption

Issues

- **Government Regulation of Encryption**
- **Import / Export of Strong Encryption**
- **Key Escrow (Both Government and Business)**
- **Encryption + Steganography = Big Trouble for Law Enforcement**
- **Privacy Issues**
- ***Many Others***

 jcavanagh@consultant-registry.com

Encryption Issues and Myths

Introduction to Encryption

Myths

- Encryption is only used by criminals or others with "something to hide".
- The longer the key, the better the encryption.
- Encryption can only be broken/overcome with a huge budget of time and computer resources.
- It is *possible* to make an unbreakable crypto scheme.
- It is *impossibl*e to make an unbreakable crypto scheme.
- A proprietary crypto scheme is more secure than a publically "vetted" scheme because the details are secure.
- *Many, many others …*

 jcavanagh@consultant-registry.com

Encryption and Business

Introduction to Encryption

What are the Business Issues of Encryption?

- Businesses Can and Do Use Encryption
  - Security/Privacy/Non-Repudiation of Financial Transaction over Networks
  - Privacy of Confidential Company Information
  - Protection against Hackers and Competition
- Issues
  - Import / Export Issues
  - Management of Employee Keys
  - Complexity of IP Sec / PKI
  - Using Crypto in Proper Balance with Ease of Use, Productivity and Sharing
  - Lack of Real Expertise
  - Outsourcing / Managed Services

 jcavanagh@consultant-registry.com

Conclusion

Introduction to Encryption

- Encryption has been around a long time
- Two Major Objectives
  - –Information Privacy/Confidentiality
  - –Source Authentication
- There are Valid Business Applications of Encryption
- There are numerous MAJOR issues in applying Encryption solutions to Business Problems!

 jcavanagh@consultant-registry.com

The End

Thanks for Watching!

For additional information or to arrange
for a security or encryption presentation,
class, or consultation
for your organization please contact:

Karen Kaye
+1.770.263.7675
kkaye@consultant-registry.com

Additional network and infrastructure security information is available at:
www.consultant-registry.com

The encrypted message is:
LRWDJWEPOJRLDTACEQAVDVFRXIFXHCFXHJOBEJBLTGSW

 jcavanagh@consultant-registry.com