

Conventional Encryption Message Confidentiality

Slides modified from Henric Johnson
Blekinge Institute of Technology, Sweden



Comp 6370 – Lecture 2 – Conventional Encryption



1

This course is important

- Computer and Network Security is the antithesis of information warfare.

"War is a matter of vital importance to the State; the province of life or death; the road to survival or ruin. It is mandatory that it be thoroughly studied."

Sun-Tzu



Comp 6370 – Lecture 2 – Conventional Encryption



2

Administrative Comments

- Honor
- Unless otherwise specified, all work is an individual effort.
- Documentation of Written Work
- Late Penalties
- Project Suggestions
- Other questions
 - Cumulative Exams?
 - Sharing Notes?
- Pacing the course



Comp 6370 – Lecture 2 – Conventional Encryption



3

Permissions

- Permissions
- Work is not turned in until the permissions are correct.
- You can ensure your permissions are correct by executing the following command:

```
chmod 777 /class/comp6370/<directory>/<filename>  
rwx = 4+2+1
```

Verify permissions by executing:

```
ls -al /class/comp6370/hw2/taylorb_hw2.txt.pgp
```



Comp 6370 – Lecture 2 – Conventional Encryption



4

Factoring Primes

- Homework 3
- Key Generation/Public Key Systems
- Factoring means finding a number's prime factors
 - Product of 2 primes – $5 * 7 = 35$
 - 35 factors into $5 * 7$.
 - $10 = 2 * 5$
 - $60 = 2 * 5 * 2 * 3$
- Keep this in mind for our discussion of public key systems next week.



Comp 6370 – Lecture 2 – Conventional Encryption



5

Outline

- Conventional Encryption Principles
- Conventional Encryption Algorithms
- Cipher Block Modes of Operation
- Location of Encryption Devices
- Key Distribution



Comp 6370 – Lecture 2 – Conventional Encryption



6

Snake-Oil Cryptography (Matt Curtin)

- Check out: <http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

"Trust Us, We Know What We're Doing"

Techno-babble
 Secret Algorithms
 Revolutionary Breakthroughs
 Experienced Security Experts, Rave Reviews, and Other Useless Certificates
 Unbreakability
 One-Time-Pads
 Algorithm or product X is insecure
 Recoverable Keys
 Exportable from the USA
 "Military Grade"



One-Time Pads and "Venona"

<http://www.nsa.gov/docs/venona>

- One-time pad: a randomly-generated, non-repeating key (length of the key at least equal to length of the message) is used only once.
 - Perfect secrecy is achieved only with a perfect RNG.
 - Quantum events, such as those measured by a Geiger counter are believed to be the only source of truly random information.
- VENONA was the codename used for the U.S. Signals Intelligence effort to collect and decrypt the text of Soviet KGB and GRU messages from the 1940's.
 - The Soviet traffic that was ultimately read under the VENONA project spanned the years 1942-46, efforts to exploit it continued for decades.
 - This was due to the agonizingly slow and difficult process in which sometimes only one or two words at a time were wrenched grudgingly from the code
 - Soviet codebooks during the years in which the main analytic breakthroughs were made (through 1952).
 - It was not until 1953 that a photocopy of a partially burned codebook (recovered by U.S. Military Intelligence in 1945) was discovered to be related to the VENONA cryptographic systems after another cryptanalytic breakthrough.
 - These messages provided extraordinary insight into Soviet attempts to infiltrate the highest levels of the United States Government.

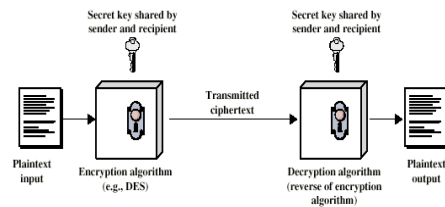


Conventional Encryption Principles

- An encryption scheme has five ingredients:
 - Plaintext
 - Encryption algorithm
 - Secret Key
 - Ciphertext
 - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm



Conventional Encryption Principles



Simplified Model of Conventional Encryption -- Stallings



Cryptography

- Classified along three independent dimensions:
 - The type of operations used for transforming plaintext to ciphertext
 - The number of keys used
 - symmetric (single key)
 - asymmetric (two-keys, or public-key encryption)
 - The way in which the plaintext is processed



Average time required for exhaustive key search

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/ μ s
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years



Feistel Cipher Structure

- Virtually all conventional block encryption algorithms, including DES have a structure first described by Horst Feistel of IBM in 1973
- The realization of a Feistel Network depends on the choice of the following parameters and design features (see next slide):
- Choice of permutation classifies algorithms of this class.

Comp 6370 – Lecture 2 – Conventional Encryption

Feistel Cipher Structure

- **Block size:** larger block sizes mean greater security
- **Key Size:** larger key size means greater security
- **Number of rounds:** multiple rounds offer increasing security
- **Subkey generation algorithm:** greater complexity will lead to greater difficulty of cryptanalysis.
- **Fast software encryption/decryption:** the speed of execution of the algorithm becomes a concern

Comp 6370 – Lecture 2 – Conventional Encryption

Inputs to the encryption algorithm:
plaintext block of 2w bits
a key K

Plaintext block is divided into two halves: L_0 and R_0

The 2 halves pass through n rounds of processing & combine to form the ciphertext block

Each round i has as inputs L_{i-1} & R_{i-1} , derived from the previous round as well as subkey K_i , derived from the overall K .

All rounds have same structure

A substitution is performed on the left half of the data by applying a round function F to the right half of the data and then taking the XOR of the output of F and the left half of the data.

The round f F is parameterized by the round subkey K_f

Classical Feistel Network – Stallings

Comp 6370 – Lecture 2 – Conventional Encryption

Conventional Encryption Algorithms

- Data Encryption Standard (DES)
 - The most widely used encryption scheme
 - The algorithm referred to is the Data Encryption Algorithm (DEA)
 - DES is a block cipher
 - The plaintext is processed in 64-bit blocks
 - The key is 56-bits in length
- A note from Stallings on DEA, DES, TDEA and 3DES:

The terminology is a bit confusing. Until recently, the terms DES and DEA could be used interchangeably. However, the most recent edition of the DES document includes a specification of the DEA described here plus the triple DEA (TDEA). Both DEA and TDEA are part of the data encryption standard. Further, until the recent adoption of the official term TDEA, the triple DEA algorithm was typically referred to as triple DES and written as 3DES.

Comp 6370 – Lecture 2 – Conventional Encryption

Longer plaintext processed in 64-bit blocks

1. Initial permutation that rearranges the bits
2. 16 iterations of the same function the 16th iteration consists of 64 bits that are a function of the input plaintext and the key.
3. Both halves are swapped to produce the pre-output

Finally, the preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation to produce the 64-bit ciphertext.

General Depiction of DES Encryption Algorithm – Stallings

Comp 6370 – Lecture 2 – Conventional Encryption

32 bits

L_{i-1}

32 bits

R_{i-1}

28 bits

C_{i-1}

28 bits

D_{i-1}

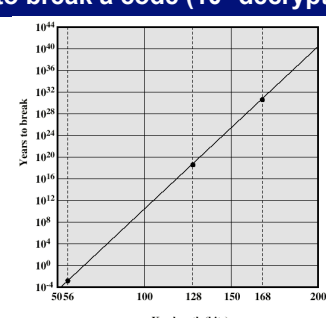
Single Round of DES Algorithm – Stallings

DES

- The overall processing at each iteration:
 - $L_i = R_{i-1}$
 - $R_i = L_{i-1} \otimes F(R_{i-1}, K_i)$
- Concerns about:
 - The algorithm and the key length (56-bits)
 - No PUBLISHED weaknesses found in the algorithm
 - 1998 – DES cracker machine built
 - cost = \$250,000
 - attack length = 3 days

Comp 6370 – Lecture 2 – Conventional Encryption

Time to break a code (10^6 decryptions/ μ s)



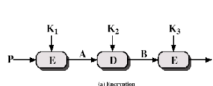
Key length (bits)	Years to break
56	10^{-4}
128	10^2
168	10^{12}

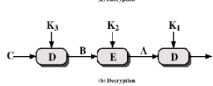
Comp 6370 – Lecture 2 – Conventional Encryption

Triple DEA

- Use three keys and three executions of the DES algorithm (encrypt-decrypt-encrypt)
 - decrypt stage only for legacy DES decryption

$$C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$$





- Effective key length of 168 bits
- RFC 3217

Comp 6370 – Lecture 2 – Conventional Encryption

Other Symmetric Block Ciphers

- International Data Encryption Algorithm (IDEA)
 - 128-bit key
 - For the round function uses XOR, addition of 16-bit integers and binary multiplication of 16-bit integers.
 - These functions are combined in such a way as to produce a complex transformation that is very difficult to analyze and hence very difficult to cryptanalyze.
 - Subkey generation algorithm relies solely on circular shifts in a complex way in order to generate six subkeys for each of the eight rounds of IDEA.
- Blowfish
 - Easy to implement
 - High execution speed
 - Run in less than 5K of memory
 - Uses dynamic S-boxes
 - Subkeys and S-boxes produced by repeated application of the Blowfish algorithm to the key
 - A total of 521 executions of the Blowfish algorithm are required to produce subkeys and S-boxes.
 - not suitable for applications where secret key frequently changes

Comp 6370 – Lecture 2 – Conventional Encryption

Other Symmetric Block Ciphers (RC-5)

- RC5 (defined in RFC 2040)
 - Suitable for hardware and software
 - uses only computational primitives
 - Fast, simple
 - works on full data words
 - Adaptable to processors of different word lengths
 - # of bits in a word is a parameter of RC5– different lengths result in different implementations
 - Variable number of rounds
 - also a parameter, allow for trade-offs between speed and security
 - Variable-length key
 - Low memory requirement
 - smart cards and other restricted memory media
 - High security (with appropriate parameters)
 - Data-dependent rotations
 - Circular bit shifts whose amount is data dependent. This appears to strengthen the algorithm

Comp 6370 – Lecture 2 – Conventional Encryption

CAST-128

- Cast-128 (defined in RFC 2144)
 - Key size from 40 to 128 bits (8 bit increments)
 - The round function differs from round to round
 - Uses fixed S-boxes
 - longer than those in DES
 - nonlinear and believed further resistant to cryptanalysis
 - S-boxes used to generate sub-keys

Comp 6370 – Lecture 2 – Conventional Encryption

Conventional Encryption Algorithms

Algorithm	Key Size	Number of Rounds	Mathematical Operations	Applications
DES	56 Bits	16	XOR, fixed S-boxes	SET Kerberos
Triple DES	112 or 168 Bits	48	XOR, fixed S-boxes	Financial Key PGP S/MIME
IDEA	126	16	XOR, variable S boxes, add	
Blowfish	40 - 448	16	Add. Sub. XOR, rotation	
CAST-128	40 to 128 bits	16	Add. Sub. XOR, rotation, fixed S-boxes	PGP

Comp 6370 – Lecture 2 – Conventional Encryption



25

Cipher Block Modes of Operation

- Cipher Block Chaining Mode (CBC)
 - The input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block.
 - Repeating pattern of 64-bits are not exposed

Equations below verifies the following illustration --

$$C_i = E_k[C_{i-1} \oplus P_i]$$

$$D_k[C_i] = D_k[E_k(C_{i-1} \oplus P_i)]$$

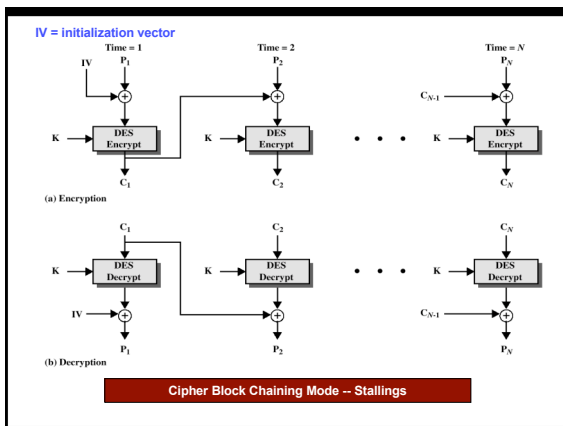
$$D_k[C_i] = (C_{i-1} \oplus P_i)$$

$$C_{i-1} \oplus D_k[C_i] = C_{i-1} \oplus C_{i-1} \oplus P_i = P_i$$

Comp 6370 – Lecture 2 – Conventional Encryption



26



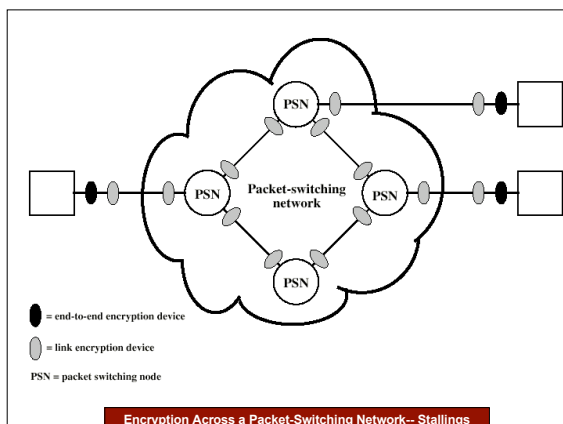
Location of Encryption Device

- Link encryption:
 - A lot of encryption devices
 - High level of security
 - Decrypt each packet at every switch
- End-to-end encryption
 - The source encrypt and the receiver decrypts
 - Payload encrypted
 - Header in the clear
- High Security: Both link and end-to-end encryption are needed

Comp 6370 – Lecture 2 – Conventional Encryption



28



Key Distribution

1. A key could be selected by A and physically delivered to B.
2. A third party could select the key and physically deliver it to A and B.
3. If A and B have previously used a key, one party could transmit the new key to the other, encrypted using the old key.
4. If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

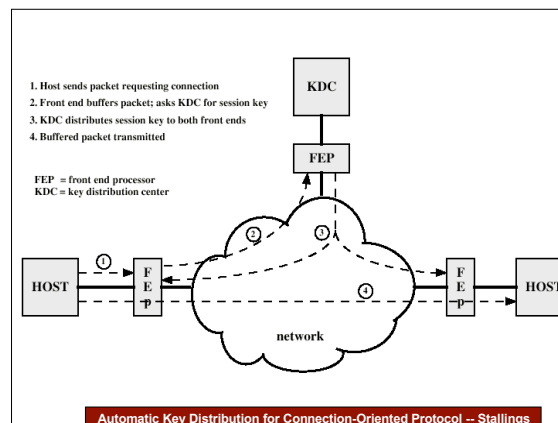
Comp 6370 – Lecture 2 – Conventional Encryption



30

Key Distribution

- **Session key:**
 - Data encrypted with a one-time session key. At the conclusion of the session the key is destroyed
- **Permanent key:**
 - Used between entities for the purpose of distributing session keys



Recommended Reading

- Stallings, W. *Cryptography and Network Security: Principles and Practice, 2nd edition*. Prentice Hall, 1999
- Schneier, B. *Applied Cryptography*, New York: Wiley, 1996
- Mel, H.X. Baker, D. *Cryptography Decrypted*. Addison Wesley, 2001

