Cryptography and Network Security

TRIPLE DES

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	6 July 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Introduction
- Triple DES
- Summary
- Test your understanding
- References

Introduction

- A replacement for DES was needed
  - theoretical attacks that can break it
  - demonstrated exhaustive key search attacks
- AES is a new cipher alternative
- Before AES alternative
  - use multiple encryptions with DES
- Triple-DES is the chosen form

Agenda

- Introduction
- Triple DES
- Summary
- Test your understanding
- References

Triple DES

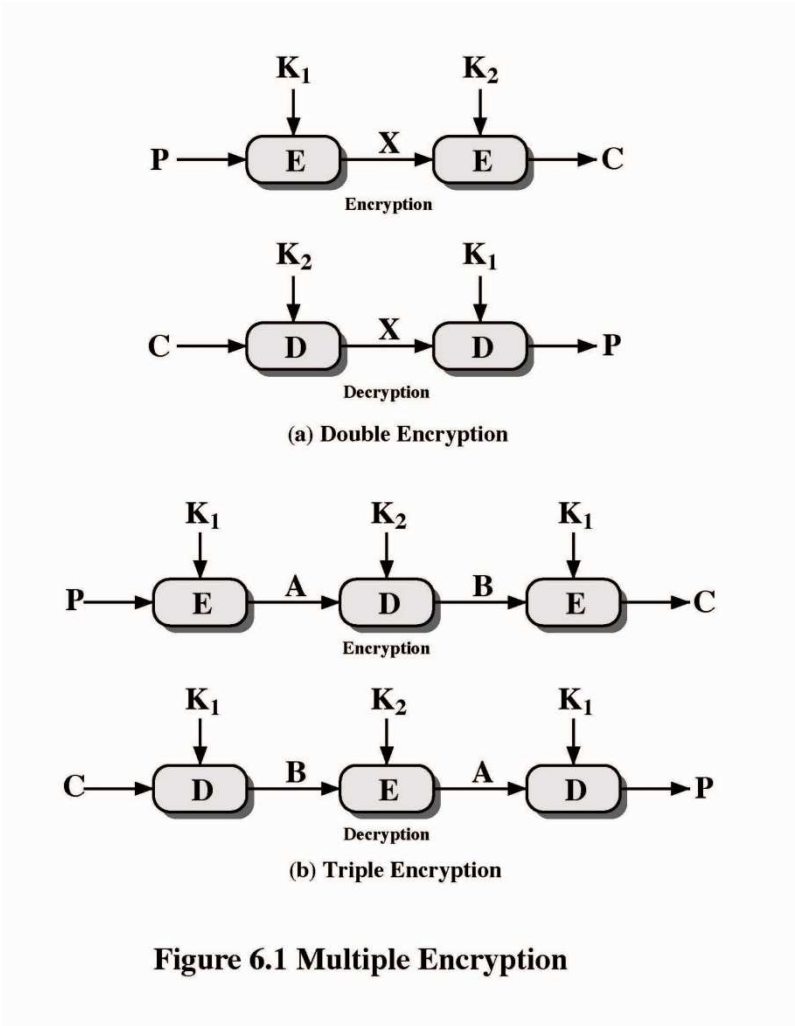

Figure 6.1 Multiple Encryption

Why Triple-DES?

- why not Double-DES?
  - NOT same as some other single-DES use, but have
- meet-in-the-middle attack
  - works whenever use a cipher twice
  - since $X = E_{K1}[P] = D_{K2}[C]$
  - attack by encrypting P with all keys and store
  - then decrypt C with keys and match X value
  - can show takes $0(2^{56})$ steps

Triple-DES with Two-Keys

- hence must use 3 encryptions
  - would seem to need 3 distinct keys
  - Key of 56 X 3 = 168 bits seems too long
- but can use 2 keys with E-D-E sequence
  - $C = E_{K1}[D_{K2}[E_{K1}[P]]]$
  - No cryptographic significance to the use of D in the second step
- standardized in ANSI X9.17 & ISO8732
- no current known practical attacks
  - some are now adopting Triple-DES with three keys for greater security

Triple-DES with Three-Keys

- although are no practical attacks on two-key Triple-DES have some indications
- can use Triple-DES with Three-Keys to avoid even these
  - $C = E_{K3}[D_{K2}[E_{K1}[P]]]$
- has been adopted by some Internet applications

Agenda

- Introduction
- Triple DES
- Summary
- Test your understanding
- References

Summary

- For stream ciphers
  - For applications that require encrypt/ decrypt of a stream of data
  - Examples: data communication channel, browser/ web link
- For block ciphers
  - For applications dealing with blocks of data
  - Examples: File transfer, e-mail, database

Agenda

- Introduction
- Triple DES
- Summary
- Test your understanding
- References

Test your understanding

1. Explain Triple DES in detail.
2. Explain meet-in-the-middle attack.
3. Briefly explain triple DES with two keys.

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.