Lecture 9: Using Block and Stream Ciphers for Secure Wired and WiFi Communications

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

April 13, 2017

11:02am

Goals:

- To present 2DES and its vulnerability to the meet-in-the-middle attack
- To present two-key 3DES and three-key 3DES
- To present the five different modes in which a block cipher can be used in practical systems for secure communications
- To discuss stream ciphers and to review RC4 stream cipher algorithm
- To review the security problems with the WEP protocol
- To review how AES is used in WPA2 for encryption and for data integrity check

CONTENTS

	Section Title	*Page*
9.1	**Multiple Encryptions with DES for a More Secure Cipher**	3
9.2	**Double DES**	4
9.2.1	Can a Double-DES (2DES) Plaintext-to-Ciphertext Mapping be Equivalent to a Single-DES Mapping?	6
9.2.2	Vulnerability of Double DES to the Meet-in-the-Middle Attack	11
9.3	**Triple DES with Two Keys**	16
9.3.1	Possible Ways to Attack 3DES Based on Two Keys	18
9.4	**Triple DES with Three Keys**	22
9.5	**Five Modes of Operation for Block Ciphers**	24
9.5.1	The Electronic Codebook Mode (ECB)	28
9.5.2	The Cipher Block Chaining Mode (CBC)	38
9.5.3	The Cipher Feedback Mode (CFB)	40
9.5.4	The Output Feedback Mode (OFB)	43
9.5.5	The Counter Mode (CTR)	45
9.6	**Stream Ciphers**	48
9.7	**The RC4 Stream Cipher Algorithm**	52
9.8	**WEP, WPA, and WPA2 FOR WiFi Security**	57
9.8.1	RC4 Encryption in WEP and WPA and Why You Must Switch to WPA2?	61
9.8.2	Some Highly Successful Attacks on WEP	68
9.8.3	AES as Used in WPA2	85
9.9	**Homework Problems**	89

9.1: MULTIPLE ENCRYPTIONS WITH DES FOR A MORE SECURE CIPHER

- As you already know, the DES cryptographic system is now known to not be secure.

- We can obviously use AES cryptography that is designed to be extremely secure, but the world of commerce and finance does not want to give up on DES that quickly (because of all the investment that has already been in DES-related software and hardware).

- So that raises questions like: How about a cryptographic system that carries out repeated encryptions with DES? Would that be more secure?

- We will now show that whereas double DES may not be that much more secure than regular DES, we can expect triple DES to be very secure.

9.2: DOUBLE DES

- The simplest form of **multiple encryptions with DES is the double DES** that has two DES-based encryption stages **using two different keys**.

- Let's say that P represents a 64-bit block of plaintext. Let E represent the process of encryption that transforms a plaintext block into a ciphertext block. Let's use two 56-bit encryption keys K_1 and K_2 for a double application of DES to the plaintext. Let C represent the resulting block of ciphertext. We have

$$C = E(K_2,\ E(K_1,\ P))$$

$$P = D(K_1,\ D(K_2,\ C))$$

  where D represents the process of decryption.

- With two keys, each of length 56 bits, double DES in effect uses a 112 bit key. One would think that this would result in a dramatic increase in the cryptographic strength of the cipher — *at*

least against the brute-force attacks to which the regular DES is so vulnerable. Recall that in a brute force attack, you try every possible key to break the code. We will argue in Section 9.2.2 that this belief is not well founded. But first, in the next subsection, let's talk about whether double DES can be thought of as a variation on the regular DES.