# Computer Security

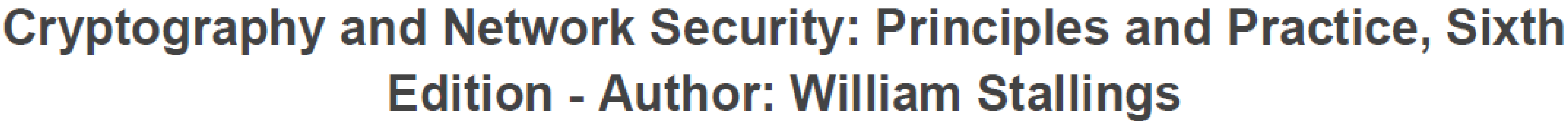
Dr. Abu Nowshed Chy

Department of Computer Science and Engineering

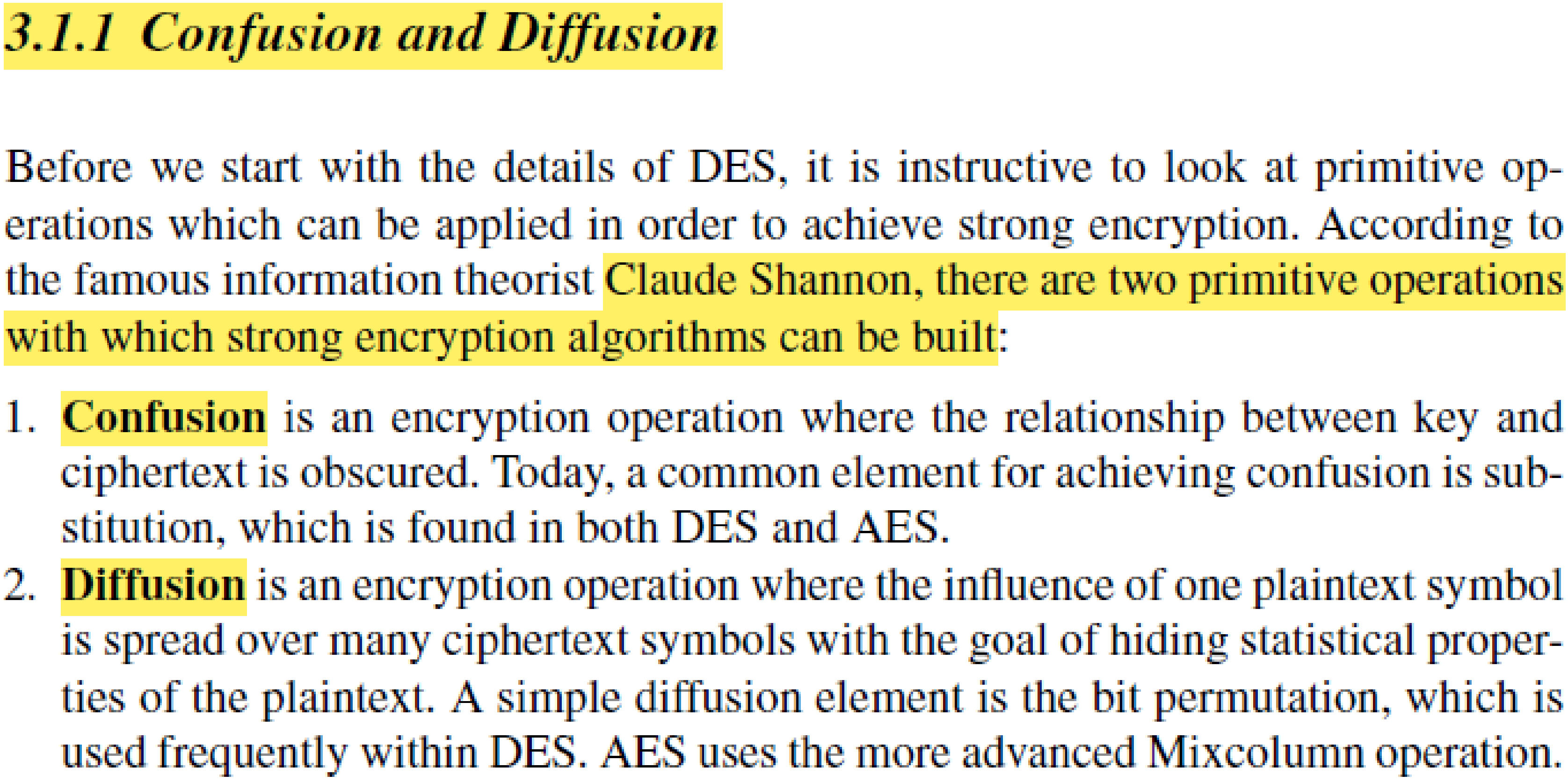
University of Chittagong

Faculty Profile

Read the pages 395 ~ 398 (13.1 Digital Signatures) from the following book:



Cryptography and Network Security: Principles and Practice, Sixth Edition - Author: William Stallings



### *3.1.1 Confusion and Diffusion*

Before we start with the details of DES, it is instructive to look at primitive operations which can be applied in order to achieve strong encryption. According to the famous information theorist Claude Shannon, there are two primitive operations with which strong encryption algorithms can be built:

1. **Confusion** is an encryption operation where the relationship between key and ciphertext is obscured. Today, a common element for achieving confusion is substitution, which is found in both DES and AES.
2. **Diffusion** is an encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext. A simple diffusion element is the bit permutation, which is used frequently within DES. AES uses the more advanced Mixcolumn operation.

### 3.3.2 The $f$-Function

As mentioned earlier, the $f$-function plays a crucial role for the security of DES. In round $i$ it takes the right half $R_{i-1}$ of the output of the previous round and the current round key $k_i$ as input. The output of the $f$-function is used as an XOR-mask for encrypting the left half input bits $L_{i-1}$.

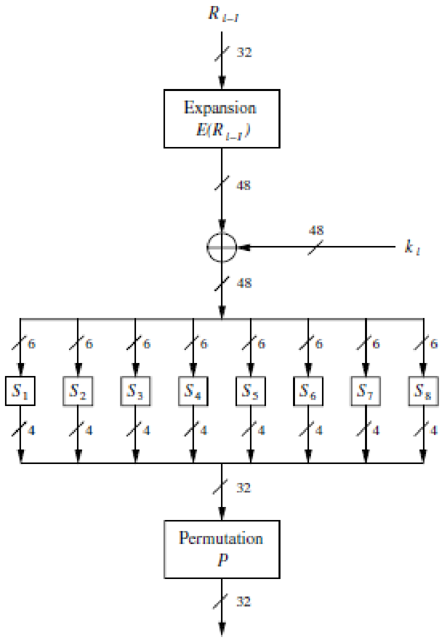


**Fig. 3.10** Block diagram of the $f$-function

# What is Network Security?

Network security allows you to take preventive measures to help protect the networking infrastructure from malfunction, misuse, destruction, modification, unauthorized access, etc. While you are uploading your data on the internet and thinking it is safe and secure, attackers can breach this data and leak confidential information or steal money. This is why it is necessary to secure your network.

Network security, is an important part of cyber security and, helps in protecting your network and data stored in it from breaches, software and hardware intrusion, and more. Network security defines a set of important rules, regulations, and configurations based on threats, network use, accessibility, and complete threat security.

# What is a Computer Virus?

A computer virus is a malicious piece of computer code designed to spread from device to device. A subset of malware, these self-copying threats are usually designed to damage a device or steal data.

Think of a biological virus – the kind that makes you sick. It’s persistently nasty, keeps you from functioning normally, and often requires something powerful to get rid of it. A computer virus is very similar. Designed to replicate relentlessly, computer viruses infect your programs and files, alter the way your computer operates or stop it from working altogether.

# How does a Computer Get a Virus?

Even if you’re careful, you can pick up computer viruses through normal Web activities like:

- Sharing music, files, or photos with other users
- Visiting an infected website
- Opening spam email or an email attachment
- Downloading free games, toolbars, media players and other system utilities
- Installing mainstream software applications without thoroughly reading license agreements

# What are the Symptoms of a Computer Virus?

Your computer may be infected if you recognize any of these malware symptoms:

- ❖ Slow computer performance
- ❖ Erratic computer behavior
- ❖ Unexplained data loss
- ❖ Frequent computer crashes

# Rogue Security Software

Leveraging the fear of computer viruses, scammers have a found a new way to commit Internet fraud.

Rogue security software is malicious software that mislead users to believe that they have network security issues, most commonly a computer virus installed on their computer or that their security measures are not up to date. Then they offer to install or update users’ security settings. They’ll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.

# Trojan Horse

Metaphorically, a “Trojan horse” refers to tricking someone into inviting an attacker into a securely protected area. In computing, it holds a very similar meaning — a Trojan horse, or “Trojan,” is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a legitimate program.

They spread often by email; it may appear as an email from someone you know, and when you click on the email and its included attachment, you’ve immediately downloaded malware to your computer. Trojans also spread when you click on a false advertisement.

Once inside your computer, a Trojan horse can record your passwords by logging keystrokes, hijacking your webcam, and stealing any sensitive data you may have on your computer.

# Adware and Spyware

By “adware” we consider any software that is designed to track data of your browsing habits and, based on that, show you advertisements and pop-ups. Adware collects data with your consent — and is even a legitimate source of income for companies that allow users to try their software for free, but with advertisements showing while using the software. The adware can slow down your computer’s processor and internet connection speed. When adware is downloaded without consent, it is considered malicious.

Spyware works similarly to adware, but is installed on your computer without your knowledge. It can contain keyloggers that record personal information including email addresses, passwords, even credit card numbers, making it dangerous because of the high risk of identity theft.

# Computer Worm

Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm spreads from an infected computer by sending itself to all of the computer’s contacts, then immediately to the contacts of the other computers.

Interestingly, they are not always designed to cause harm; there are worms that are made just to spread. Transmission of worms is also often done by exploiting software vulnerabilities. While we don’t hear about them much today, computer worm are one of the most common computer network threats.

# DOS and DDOS Attack

There are cases whenever a website's server gets overloaded with traffic and simply crashes, e.g. sometimes when a news story breaks. But more commonly, this is what happens to a website during a DoS attack, or denial-of-service, a malicious traffic overload that occurs when attackers over-flood a website with traffic. When a website has too much traffic, it's unable to serve its content to visitors.

A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. Fortunately, you can't really overload a server with a single other server or a PC anymore. In the past years it hasn't been that common if anything, then by flaws in the protocol.

# DOS and DDOS Attack

A DDoS attack, or distributed denial-of-service attack, is similar to DoS, but is more forceful. It's harder to overcome a DDoS attack. It's launched from several computers, and the number of computers involved can range from just a couple of them to thousands or even more.

Since it's likely that not all of those machines belong to the attacker, they are compromised and added to the attacker's network by malware. These computers can be distributed around the entire globe, and that network of compromised computers is called botnet.

Since the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against.

# Phishing

Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, and credit card numbers.

The attacks often come in the form of instant messages or phishing emails designed to appear legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient’s computer. It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify your identity by giving away your private information.

# Rootkit

Rootkit is a collection of software tools that enables remote control and administration-level access over a computer or computer networks. Once remote access is obtained, the rootkit can perform a number of malicious actions; they come equipped with keyloggers, password stealers and antivirus disablers.

Rootkits are installed by hiding in legitimate software: when you give permission to that software to make changes to your OS, the rootkit installs itself in your computer and waits for the hacker to activate it. Other ways of rootkit distribution include phishing emails, malicious links, files, and downloading software from suspicious websites.

# SQL Injection Attack

SQL injection attacks are designed to target data-driven applications by exploiting security vulnerabilities in the application's software. They use malicious code to obtain private data, change and even destroy that data, and can go as far as to void transactions on websites. It has quickly become one of the most dangerous privacy issues for data confidentiality.

# Clop Ransomware

Ransomware is malware which encrypts your files until you pay a ransom to the hackers. “Clop” is one of the latest and most dangerous ransomware threats. It’s a variant of the well-known CryptoMix ransomware, which frequently targets Windows users.

Before beginning the encryption process, the Clop ransomware blocks over 600 Windows processes and disables multiple Windows 10 applications, including Windows Defender and Microsoft Security Essentials — leaving you with zero chance of protecting your data.

The Clop ransomware has evolved since its inception, now targeting entire networks — not just individual devices. Even the Maastricht University in the Netherlands became a victim of the Clop ransomware, with almost all Windows devices on the university’s network being encrypted and forced to pay a ransom.

# IoT Device Attacks

As the popularity of IoT (Internet of Things) devices grows in 2022 — things like smart speakers and video doorbells — hackers are looking to exploit these devices for valuable information.

There are multiple reasons why hackers choose to target IoT devices. For one, most IoT devices don’t have enough storage to install proper security measures. These devices often contain easy-to-access data such as passwords and usernames, which then can be used by hackers to log into user accounts and steal valuable information, such as banking details.

Hackers can also use internet-based cameras and mics to spy on and communicate with people — including young children via smart baby monitors.

These devices can also act as weak points in a corporation’s network, meaning hackers can gain access to entire systems through unsecured IoT devices — spreading malware to other devices across the network.

# Computer Virus Protection

Take these steps to safeguard your PC with the best computer virus protection:

- Use antivirus protection and a firewall
- Get antispyware software
- Always keep your antivirus protection and antispyware software up-to-date
- Update your operating system regularly
- Increase your browser security settings
- Avoid questionable Websites
- Only download software from sites you trust.
- Carefully evaluate free software and file-sharing applications before downloading them.
- Don't open messages from unknown senders
- Immediately delete messages you suspect to be spam

# Thank You!