



Computer Science

Grade 10

Topics



01 Logic Gates

02 Security Issues

03 Internet Principles

Topic 1: Logic Gates

What is Logic Gates?

A logic gate is an elementary building block of a digital circuit. Most logic gates have two inputs and one output. At any given moment, every terminal is in one of the two binary conditions low (0) or (1), represented by different voltage levels.

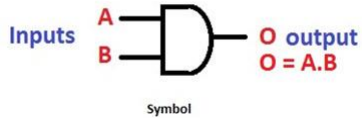
The six types of gates are named in Boolean notation as:

- OR GATE
- AND GATE
- NOT GATE
- NAND GATE
- NOR GATE
- EXOR GATE

Logic Gates

1. AND GATE

The AND gate is an electronic circuit that gives a high output (1) only if all its inputs are high

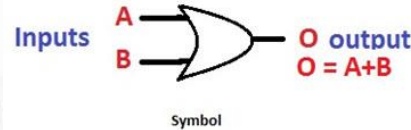


Inputs		Output
A	B	O
0	0	0
0	1	0
1	0	0
1	1	1

Truth table

2. OR GATE

The OR gate is an electronic circuit that gives a high output (1) if one or more of its inputs are high.

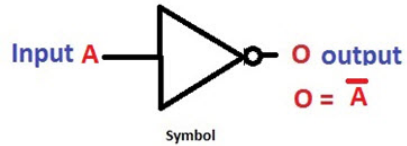


Inputs		Output
A	B	O
0	0	0
0	1	1
1	0	1
1	1	1

Truth table

3. NOT GATE

The Not gate is an electronic circuit that produces an inverted version of the input at its output. It is also known as an inverter. If the input variable is A, the inverted output is known as NOT A

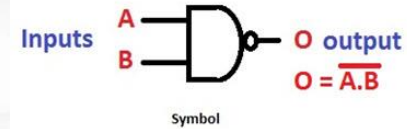


Inputs	Output
A	O
0	1
1	0

Truth table

4. NAND GATE

This is a NOT-AND gate which is equal to an AND gate followed by a NOT gate

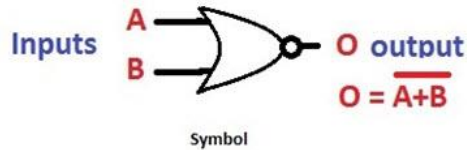


Inputs		Output
A	B	O
0	0	1
0	1	1
1	0	1
1	1	0

Truth table

5. NOR GATE

This is a NOT-OR gate which is equal to an OR gate followed by a NOT gate. The outputs of all NOR gates are low if any of the inputs are high.

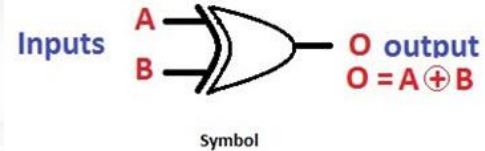


Inputs		Output
A	B	O
0	0	1
0	1	0
1	0	0
1	1	0

Truth table

6. EXOR GATE

The 'exclusive-OR' gate is a circuit which will give a high output if either, but not both, of its two inputs are high.



Inputs		Output
A	B	O
0	0	0
0	1	1
1	0	1
1	1	0

Truth table

Topic 2: Security Issues

The security aspects of using the internet is important because we have control in what we are using on the net so as not to fall into the trap of viruses.

• Virus

Viruses are malicious programs that spread throughout computer files without user knowledge. Most widespread virus infections spread through email message attachments that activate when opened. The vicious cycle of a virus perpetuates as infected emails are forwarded to multiple users. Viruses also spread through shared media, such as Universal Serial Bus (USB) drives.

Symptoms that we can notice with an infected computer:

- Slows down
- Runs short of memory
- Files can be corrupted or deleted
- Computer shut down intermediately

In order to remove viruses, we need to take actions:

- Install regularly updated anti viruses
- Do not buy pirated versions of software, buy originals
- On internet, visit secured sites

- **Malware**

Malware is a file or program other than a virus that is potentially harmful. Many malware attacks are phishing attacks, which try to persuade the user to unknowingly give attackers access to personal information. As you fill out an online form, the data is sent to the attacker. Malware can be removed using spyware and adware removal tools.

- **Spyware**

Spyware is similar to adware. It is distributed without any user intervention or knowledge . After it is installed the spyware monitors activity on the computer. The spyware then sends this information to the organisation responsible for launching the spyware.

- **Phishing**

Phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and social security numbers.



- **Pharming**

Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent.

- **Spamming**

Electronic spamming is the use of electronic messaging systems to send an unsolicited message (spam), especially advertising as well as sending messages repeatedly on the same site.

- **Hacking**

Hacking refers to the act of gaining illegal access to a computer system with the intention to cause harm. A hacker is someone who often uses techniques to break into computer systems by cracking passwords.

HOW DATA ARE KEPT SAFE

There are several methods used to protect data, which include:

- **Password** a secret code which is used to gain access to a system . Password can either be typed using a keyword or using biometrics. Biometrics means to measure and analyze some human characteristics in order to correctly identify an individual
- A **firewall** is a hardware or software that is used to protect a computer or private network resources from intruders or hackers
- **Symmetric encryption** (or pre-shared key encryption) uses a single key to both encrypt and decrypt data. Both the sender and the receiver need the same key to communicate
- **Secure Socket Layer** (SSL) and **Transport Layer Security**(TLS) are standard security technologies for establishing an encrypted link between server and a client, typically a website and a browser or a mail server and a mail client

Topic 3: Internet Principles

What is Web Browsers?

A web browser, or simply "browser," is an application used to access and view websites.

Common web browsers include:

- Microsoft Internet Explorer
- Google Chrome
- Mozilla Firefox
- Apple Safari



What is Internet Service Provider?

A company that provides you with access to the Internet, usually for a fee.

The most common ways to connect to an ISP are by using a phone line (dial-up) or broadband connection (cable or DSL).

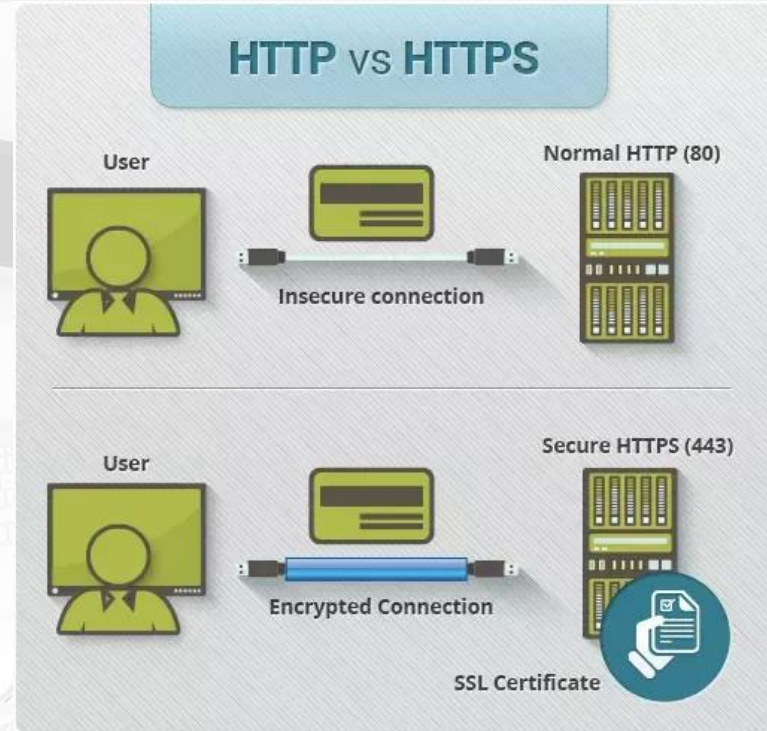


What is http?

Hypertext transfer protocol (http) is the underlying protocol used by the World Wide Web which defines (1) how messages are formatted and transmitted, and (2) what actions Web servers and browsers should take in response to various commands.

What is https?

Hypertext transfer protocol over secure (https) is a secure method of accessing or sending information across a web page. All data is encrypted before it is sent, preventing anyone from understanding that information if intercepted.



What is HTML?

HyperText Markup Language (HTML) is the markup language used in creating web pages on the World Wide Web.

Distinguish between HTML structure and presentation

- HTML structure consists of the statements that contains content / the structural mark-up of a webpage
- HTML presentation alters the style of the content e.g. CSS

This is HTML structure

```
<section><p style="color: red;">The presentation is created by the style command</p>
</section>
```

What is a URL?

URL is the abbreviation of Uniform Resource Locator and is defined as the global address of documents and other resources on the World Wide Web.

`http://www.steves-internet-guide.com/understanding-web-address/`

↑
Protocol

↑
Domain Name

↑
Path to file

Media Access Control (MAC)

Media Access Control (MAC) address is a **unique id** for the network interface card on a particular network

- It is stored in hexadecimal. e.g. **00-15-E9-2B-99-3C**
- First six digits are the **manufactures' code**
- Last six digits are the **serial number** of the device

IP Address

- Internet Protocol (IP) combined with TCP (transmission control protocol) is the method used to send data to the **correct address**.
- Every computer on a network has a unique IP address. e.g. **207.218.171**
- Composed of **four integers/bytes** each in the range **0 – 255** (hex: 00-FF)

Cookies

- Cookies are small, **encoded, text files** that contain data that is used to help you navigate through a particular website each time you log on.
- Cookies are able to distinguish between new and **repeat visitors** to the website.
- Cookies are **generated by the website** you are visiting and stored in your browser's folder.
- Helps implement shopping carts and **one-click purchasing**.
- Cookies can be used to **track** your browser's website browsing history, which concerns some users.