

Homeworks with Modern Tools and Concepts

CSE487 Cybersecurity, Law and Ethics

[Week 1 Homework 1. Caesar Cipher Implementation](#)

[Week 1 Homework 2. MTU is Maximum Transmission Unit](#)

[Week 2 Homework 3. Implement at least three cipher algorithms of different types.](#)

[Week 2 Homework 4. Working with a virtual machine](#)

[Week 2 Homework 5. Complete the Linux Fundamentals Part 1](#)

[Week 2 Homework 6. Pass up to level 14 in Bandit Wargame](#)

[Week 2 Homework 7. Configure root CA, sub CA, and a server that uses https://](#)

[Week 3 Homework 9. Configure a Web server](#)

[Week 3 Homework 8. Configure a DNS server](#)

[Week 3 Homework 9. Password Cracking](#)

[Week 3 Homework 10. Apply Mask attack on the hash using hashcat.](#)

[Week 3 Homework 11. Understand the basics and problems of Diffie-Hellman Key Exchange](#)

[Week 3 Homework 12: Familiarize yourself with the Cryptography library](#)

[Week 4 Homework 13: Understanding the RSA Algorithm](#)

[Week 4 Homework 14: Steganography](#)

[Week 4 Homework 15. Understanding TLS and decrypting HTTPS traffic](#)

[Week 4 Homework 16. Extract the values of the exponent and modulus from the SSL certificate](#)

[Week 5 Homework 17: Practical Cryptography Requirements](#)

[Week 5 Homework 18: Modern Encryption and Digital Signatures](#)

[Week 5 and onward: Project: Public Key Infrastructure Implementation](#)

[Attack Glossary:](#)

[Law and Ethics Part](#)

[Mini Project-3: Present an ethical dilemma in decision making in the field of IT.](#)

[Knowledgebase](#)

[Hash Functions](#)

Concepts

<Midterm-1>

Open a Repository on Github, and create folders for each of the assignments you work on.

Write documentations and create demos of your project on YouTube.

Week 1 Homework 1. Caesar Cipher Implementation

Resources:

[Caesar Cipher in Python - Javatpoint](#)

[Caesar Cipher in Cryptography - GeeksforGeeks](#)

[Cryptography with Python - Caesar Cipher](#)

[Caesar Cipher In Python \(Text Encryption Tutorial\) - Like Geeks](#) [*best*]

[Python: Create a Caesar encryption - w3resource](#) [*with step-by-step visualization*]

Tasks:

1. Implement Caesar Cipher in any programming language.
cipher_text = caesar_cipher (plain_text, shift)
2. Break the cipher using brute force (i.e., trying all possible combinations).
3. Attempt to break the cipher using **cryptanalysis** (e.g., perform letter frequency analysis on the ciphertext and try to match with the letter frequency in English Language). How can you be sure that you found the right key? [*challenging-task*]

Delivery: Demonstrate your work while recording the screen, upload the video on YouTube.

Deadline: None. However, it is expected that you complete the tasks by the first week.

Week 1 Homework 2. MTU is Maximum Transmission Unit

1. Write a computer program to discover the actual MTU size of your communication network.

[Find a Path's MTU using PING Command Windows, Linux, Etc](#)

2. What is the difference between MTU and MSS?

<https://youtu.be/XMcYwr-yJGA>

<https://youtu.be/XMcYwr-yJGA>

3. Compare the discovered MSS with the MTU size displayed in your operating system. Explain the reason, with a diagram.

netsh command

```
#netsh interface ipv4 show subinterfaces
```

Information: 2021 Facebook Outage

📺 Facebook, Instagram and WhatsApp down in global outage

<https://www.youtube.com/watch?v=g2rk1MA-aLU>

📺 Why was Facebook down for five hours?

<https://www.youtube.com/watch?v=wMU8vmfaYo&t=520s>

📺 Why Did Facebook Go Down? - Computerphile

<https://www.youtube.com/watch?v=Bie32IZIMtY>

Facebook's explanation: [More details about the October 4 outage - Engineering at Meta](https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/)
<https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/>

Learn about Interior Gateway Protocols and Exterior Gateway Protocols. What kind of protocol is BGP? What is an AS Number? How is it related to BGP?

Week 2 Homework 3. Implement at least three cipher algorithms of different types.

Difference between Monoalphabetic Cipher and Polyalphabetic Cipher
<https://www.geeksforgeeks.org/difference-between-monoalphabetic-cipher-and-polyalphabetic-cipher/?ref=lbp>

Transposition, Substitution, Monoalphabetic, [Polyalphabetic Cipher](#)

PlayFair Cipher, Polyalphabetic
One Time Pad, Vigenere Tableau,

Information: Understand the difference between encoding and encryption.

encoding is conversion. a secret key is not required.

encryption is transformation. a secret key is required. The secrecy of the encryption depends on the secrecy of the secret key (Kerckhoff's Principle) .

The reverse process of encoding is called decoding. The reverse process of encryption is called decryption.

Hash-ing is similar to encoding but it can not be decoded. When someone discovers the method of decoding a hash function, the hash function is "broken". For example, MD5 algorithm is broken, because it can be reversed.

Hash functions have some additional requirements, like fixed length output, avalanche effect, collision resistance and so on.

In class, a random student from the class will be asked to explain the **birthday attack** on the whiteboard. and how it is relevant to hashing and cracking.

Week 2 Homework 4. Working with a virtual machine

1. Install Oracle Virtualbox or VMWare.
2. Download and install Xubuntu/Lubuntu/Linux Mint/Kali/Parrot/Debian or any other linux distro (debian-based systems preferred). Do not choose Kali Linux if your computer is of low configuration.
3. Take a snapshot (not screenshot) of the virtual machine and save it as "State 0".
4. Delete everything in the computer with the following command as root.

```
# sudo rm -rf /*
```
5. And enjoy your beloved machine being destroyed in front of your eyes.
6. Restore the snapshot taken earlier which was saved as "State 0".

7. Run update and upgrade:
sudo apt-get update && sudo apt-get upgrade
sudo apt-get dist-upgrade
8. Configure the network of the virtual machine to use a **host-only network**. Understand the difference among Bridged Adapter, NAT, Host-only network configurations.
9. Host-only networks have the ip address in the 192.168.56.0/24 subnet. Note down the IPv4 address of the virtual machine in a host-only network with the command
~ ip addr or ~ ifconfig
10. Change the hostname of the VM to "server".
11. Clone the virtual machine, turn it on and change the hostname to "client".
12. Check if the client (i.e., the cloned VM) also configured to use the host-only network.
13. Ping from the server to the client and vice-versa to check the connectivity.

Week 2 Homework 5. Complete the Linux Fundamentals Part 1

[TryHackMe | Linux Fundamentals Part 1](https://tryhackme.com/room/linuxfundamentalspart1)

<https://tryhackme.com/room/linuxfundamentalspart1>

Week 2 Homework 6. Pass up to level 14 in Bandit Wargame

[OverTheWire: Bandit](https://overthewire.org/wargames/bandit/)

<https://overthewire.org/wargames/bandit/>

Solution and Walkthrough:

[OverTheWire - Bandit Walkthrough](https://home.adelphi.edu/~ni21347/cybersecgames/OverTheWire/Bandit/index.html)

<https://home.adelphi.edu/~ni21347/cybersecgames/OverTheWire/Bandit/index.html>

[OverTheWire-Wargames-Bandit Walkthrough | by Kanishka | Medium](https://medium.com/@Kan1shka9/overthewire-wargames-bandit-walkthrough-df2b86826c67)

<https://medium.com/@Kan1shka9/overthewire-wargames-bandit-walkthrough-df2b86826c67>

[OverTheWire – Bandit Walkthrough \(1-14\) - Hacking Articles](https://www.hackingarticles.in/overthewire-bandit-walkthrough-1-14/)

<https://www.hackingarticles.in/overthewire-bandit-walkthrough-1-14/>

[Over The Wire: WARGAMES;Bandit level 0 to 10 WALKTHROUGH | Medium | InfoSec Write-ups](https://infosecwriteups.com/over-the-wire-wargames-bandit-level-0-to-10-walkthrough-97015bfc6538)

<https://infosecwriteups.com/over-the-wire-wargames-bandit-level-0-to-10-walkthrough-97015bfc6538>

Week 2 Homework 7. Configure root CA, sub CA, and a server that uses https://

Become a master of OpenSSL  Masterclass in openssl

<https://www.youtube.com/watch?v=d8OpUcHzTeg>

Useful tools:

XCA (OpenSSL GUI)

<https://hohnstaedt.de/xca/index.php/download>

X - Certificate and Key management: This application is intended for creating and managing X.509 certificates, certificate requests, RSA, DSA and EC private keys, Smartcards and CRLs.

Everything that is needed for a CA could be done with XCA (instead of OpenSSL).

Week 3 Homework 9. Configure a Web server

Install and configure Apache2.

[Install and Configure Apache | Ubuntu](https://ubuntu.com/tutorials/install-and-configure-apache)

<https://ubuntu.com/tutorials/install-and-configure-apache>

[How To Install the Apache Web Server on Ubuntu 22.04 | DigitalOcean](https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-22-04)

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-22-04>

Learn more about server hardening:

[How to-Ubuntu Hardening Security Best Practices Checklist](https://gist.github.com/mirajehossain/59c6e62fcdc84ca1e28b6a048038676c)

<https://gist.github.com/mirajehossain/59c6e62fcdc84ca1e28b6a048038676c>

<https://github.com/konstruktoid/hardening>

<https://dewapost.com/2022/03/19/how-to-hardening-the-ubuntu-server/>

Add a new user for the apache2 web service

Week 3 Homework 8. Configure a DNS server

[An Introduction to DNS Terminology, Components, and Concepts | DigitalOcean](https://www.digitalocean.com/community/tutorials/an-introduction-to-dns-terminology-components-and-concepts)

<https://www.digitalocean.com/community/tutorials/an-introduction-to-dns-terminology-components-and-concepts>

Week 3 Homework 9. Password Cracking

You want to find someone's password. But all you have is some hash value of the password.

Like: **e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f**

A hash value is also known as a "digest".

- Identify the hashing algorithm.

Try to identify the hashing algorithm from the digest length. Which one it could be?

```
len("e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f")
```

```
= 64
```

```
# So, the length is 64.
```

```
sorted(set("e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f"))
```

```
= ['0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f']
```

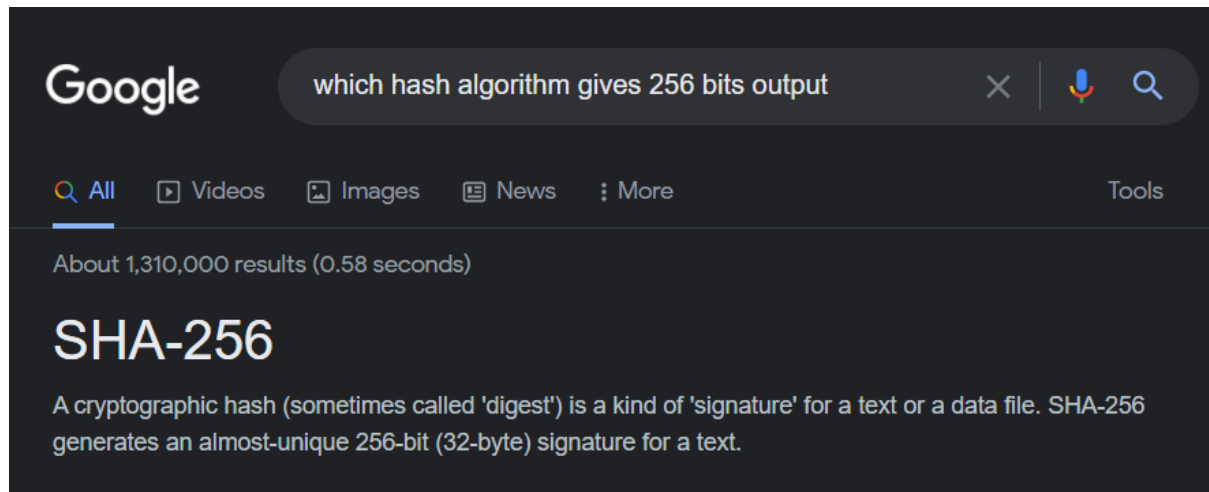
```
# So, these could be Hexadecimal values. Since, Hexadecimal is a 4-bit representation of binary, therefore the following is true:
```

```
len("e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f")
```

```
= 64 Hex Values
```

= 64 * 4 bits = 256 bits.

Ask your best friend about it:



Now you have to reverse the hash function to find out

for which *input*, this particular SHA256 value is the output?

That means, if **x** is the password, you have to find **x** where,

sha256sum(**x**) = e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f

The password could be a permutations of:

- Some or all digits of a phone number
- Some or all digits of any date (e.g., birthday, marriage day, some other day)
- Recent years/months, around the victim's birth year/month,
- Name of a person, location, school, university.
- Something relevant to the person
- Weak passwords like abc123, 123456, password, iloveyou

You can either launch a Brute Force attack or a Dictionary attack against the digest to find the password. If Brute Force is not feasible, a dictionary (wordlist) of common passwords can be used to match the hash.

So, a hash cracking program should go through each of the lines (1 word per line) and calculate the hash value for that word, and compare the digest with the given digest. Keep trying until a match is found.

1. Calculate the time required to Brute Force the password with 4000 passwords per second.
2. Generate a dictionary/wordlist using *Crunch*.
[Comprehensive Guide on Crunch Tool - Hacking Articles](https://www.hackingarticles.in/comprehensive-guide-on-crunch-tool/)
<https://www.hackingarticles.in/comprehensive-guide-on-crunch-tool/>
3. What is the dictionary size?
4. Use *Hashcat* to break the password using the dictionary created with *Crunch*.
5. How long would your system CPU or GPU take to try this wordlist to find the actual password?
You can modify your code to use the GPU if it takes too long.

6. How is “John The Ripper” relevant? Is it better or worse?
You can generate the wordlist on the fly (without generating a wordlist) using *Crunch* and pipe the output to *Hashcat*.
7. What is a “Rainbow Table”? What is a “salt”? How are these two relevant to cryptology and password cracking?
8. Understand how SHA256 is calculated. [**Bonus***]
9. Specify some modern tools for password cracking. [**Bonus***]
[Taking Password Cracking to the Next Level – CryptoKait](https://cryptokait.com/2020/09/02/taking-password-cracking-to-the-next-level/)
<https://cryptokait.com/2020/09/02/taking-password-cracking-to-the-next-level/>

Hint: Cracking a hash with hashcat:

Given that,

sha256 (“CSE487”) = e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f

The input CSE487 contains 3 uppercase characters and 3 digits. Therefore the pattern for hashcat would be:

?u?u?u?d?d?d

Where ?u denotes all UPPERCASE characters and ?d denotes all digits. Learn more from the manual of hashcat. <https://manpages.org/hashcat> or type “man hashcat” in a Linux terminal.

Install hashcat on your Windows host [virtual machines will generate error: **illegal hardware instruction**]

Week 3 Homework 10. Apply Mask attack on the hash using hashcat.

[mask_attack \[hashcat wiki\]](#)

https://hashcat.net/wiki/doku.php?id=mask_attack

Command Syntax:

hashcat -m **<hash type>** -a **<attack type>** **<hash value>** **<pattern>**

Example:

hashcat -m **1400** -a **3** **e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f**
?u?u?u?d?d?d

```
C:\Users\mcctu\Downloads\Compressed\hashcat-6.2.5>hashcat -m 1400 -a 3
e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f ?u?u?u?d?d?d
```

```
hashcat (v6.2.5) starting
```

```
OpenCL API (OpenCL 3.0 ) - Platform #1 [Intel(R) Corporation]
```

```
=====
```

```
* Device #1: Intel(R) UHD Graphics, 1536/3173 MB (793 MB allocatable), 32MCU
```

```
Minimum password length supported by kernel: 0
```

Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts

Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:

- * Zero-Byte
- * Early-Skip
- * Not-Salted
- * Not-Iterated
- * Single-Hash
- * Single-Salt
- * Brute-Force
- * Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.

Pure kernels can crack longer passwords, but drastically reduce performance.

If you want to switch to optimized kernels, append -O to your command line.

See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.

Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 579 MB

The wordlist or mask that you are using is too small.

This means that hashcat cannot use the full parallel power of your device(s).

Unless you supply more work, your cracking speed will drop.

For tips on supplying more work, see: <https://hashcat.net/faq/morework>

Approaching final keypace - workload adjusted.

e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f:CSE487

Session.....: hashcat

Status.....: Cracked

Hash.Mode.....: 1400 (SHA2-256)

Hash.Target.....: e4760b8c578faff251538fe7be740bf801161304e5b11553d76...19de6f

Time.Started.....: Thu Mar 03 19:37:21 2022 (1 sec)

Time.Estimated....: Thu Mar 03 19:37:22 2022 (0 secs)

Kernel.Feature....: Pure Kernel

Guess.Mask.....: ?u?u?u?d?d?d [6]

Guess.Queue.....: 1/1 (100.00%)


```
Speed.#1.....: 9483.3 kH/s (0.17ms) @ Accel:128 Loops:10 Thr:16 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 4342784/17576000 (24.71%)
Rejected.....: 0/4342784 (0.00%)
Restore.Point....: 6144/26000 (23.63%)
Restore.Sub.#1...: Salt:0 Amplifier:360-370 Iteration:0-10
Candidate.Engine.: Device Generator
Candidates.#1....: ZBT691 -> JSQ391
```

```
Started: Thu Mar 03 19:37:17 2022
Stopped: Thu Mar 03 19:37:24 2022
```

Week 3 Homework 11. Understand the basics and problems of Diffie-Hellman Key Exchange

Used to generate/agree upon a symmetric key in the presence of an eavesdropper.

▶ Secret Key Exchange (Diffie-Hellman) - Computerphile

<https://www.youtube.com/watch?v=NmM9HA2MQGI>

▶ Diffie Hellman -the Mathematics bit- Computerphile

https://www.youtube.com/watch?v=Yjrfm_oRO0w

▶ Diffie Hellman Key Exchange Algorithm | Complete Working with Diagram & Example

https://www.youtube.com/watch?v=xSUMEer6J_E

▶ Public key cryptography - Diffie-Hellman Key Exchange (full version)

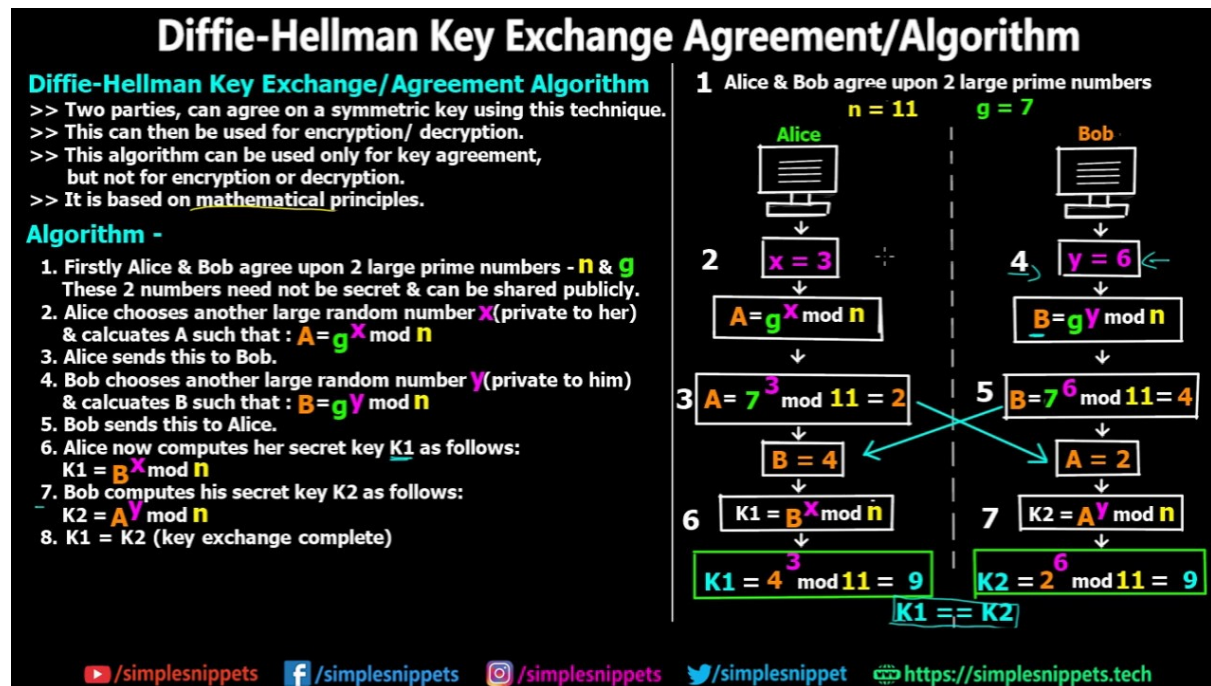
https://www.youtube.com/watch?v=YEBfamv-_do

▶ Public Key Cryptography: Diffie-Hellman Key Exchange (short version)

<https://youtu.be/3QnD2c4Xovk>

▶ Gambling with Secrets: Part 7/8 (Diffie-Hellman Key Exchange)

<https://www.youtube.com/watch?v=6NcDVERzMGw>



Week 3 Homework 12: Familiarize yourself with the Cryptography library

How to Encrypt and Decrypt Data in Python using Cryptography Library

<https://devqa.io/encrypt-decrypt-data-python/>

How to Encrypt and Decrypt Strings in Python?

<https://www.geeksforgeeks.org/how-to-encrypt-and-decrypt-strings-in-python/>

How to calculate hash using hashlib

[SHA256 Encryption with Python by Josh Dwernychuk | Medium](https://medium.com/@dwnrychukjosh/sha256-encryption-with-python-bf216db497f9)

<https://medium.com/@dwnrychukjosh/sha256-encryption-with-python-bf216db497f9>

```
import hashlib

def hash(string):
    sha_signature = hashlib.sha256(string.encode()).hexdigest()
    return sha_signature

string = 'CSE487'
sha_signature = hash(string)
print(sha_signature)

# e4760b8c578faff251538fe7be740bf801161304e5b11553d76a10e79219de6f
```

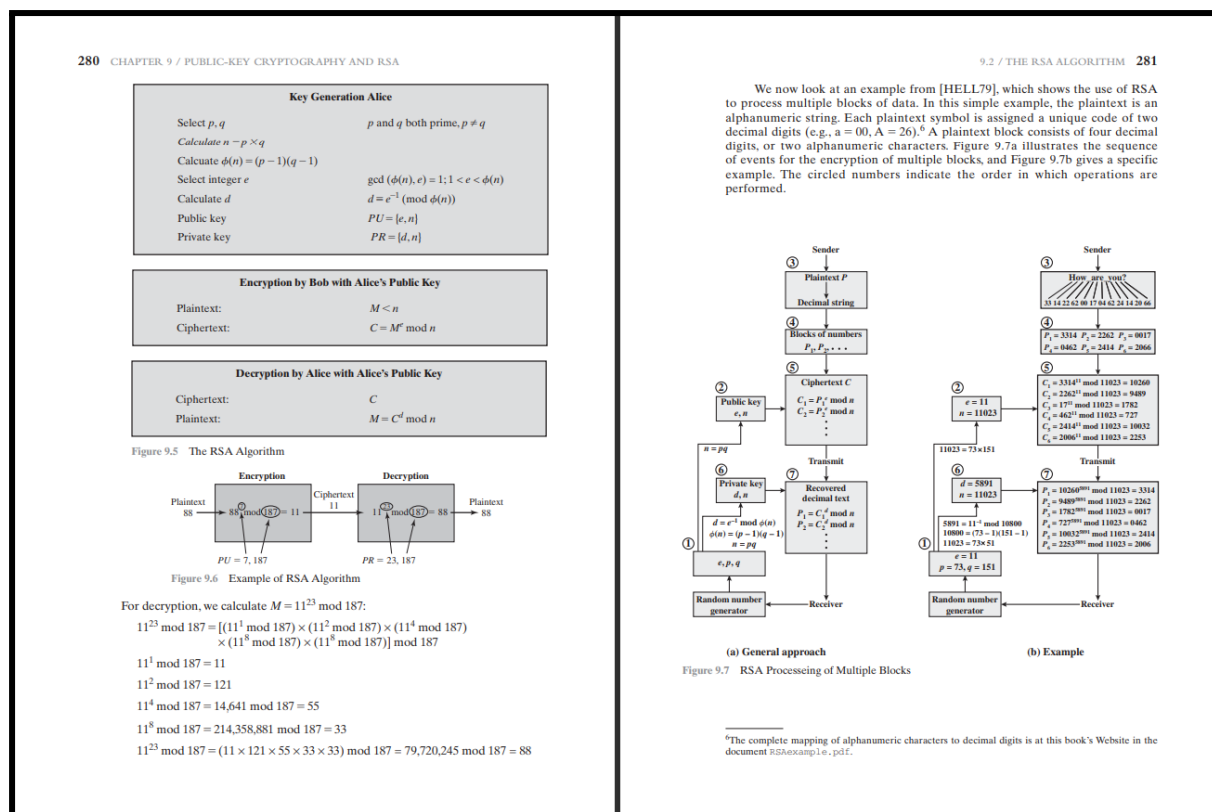
Information: Understanding Encryption

[Gambling with Secrets \(Cryptography\) - YouTube](https://www.youtube.com/watch?v=PLB4D701646DAF0817)

<https://www.youtube.com/playlist?list=PLB4D701646DAF0817>

Week 4 Homework 13: Understanding the RSA Algorithm

Read section 9.2 of the Cryptography and Network Security by William Stallings



https://umaranis.com/rsa_calculator_demo.html

RSA Calculator

<https://www.cs.drexel.edu/~jpopack/IntroCS/HW/RSASWorksheet.html>

Online RSA key generation

https://www.mobilefish.com/services/rsa_key_generation/rsa_key_generation.php

RSA Cipher

<https://www.dcode.fr/rsa-cipher>

Week 4 Homework 14: Steganography

LSB steganography:

<https://github.com/livz/cloacked-pixel>

Reliable detection of LSB Steganography is still a problem.

<https://github.com/RobinDavid/LSB-Steganography>

Python program based on steganographic methods to hide files in images using the Least Significant Bit technique.

[Steganography - A list of useful tools and resources - 0xRick's Blog](#)

<https://0xrick.github.io/lists/stego/>

OpenStego for Data Hiding and Digital Watermarking


<https://www.openstego.com/> [requires java]

Concepts: <https://www.openstego.com/concepts.html>

Tutorial: [Conceal Any Data with OpenStego](#)

<https://medium.com/codex/conceal-any-data-with-openstego-7dcc908d3497>

Week 4 Homework 15. Understanding TLS and decrypting HTTPS traffic

 Analyzing TLS session setup using Wireshark

<https://www.youtube.com/watch?v=MQg48n9IV0s>

Decrypting HTTPS (SSL/TLS+HTTP):

<https://www.comparitech.com/net-admin/decrypt-ssl-with-wireshark/>

Week 4 Homework 16. Extract the values of the exponent and modulus from the SSL certificate

Open the SSL certificate by clicking on the Padlock icon in the address bar of your browser. Export the certificate as "ewubd SSL cert.cer". By default, Windows exports it as a DER formatted file with *.cer extension, but it needs to be converted to PEM format. Then OpenSSL can extract the public key from the PEM formatted certificate.

The public key can be extracted from the certificate "ewubd SSL cert.cer" (in DER format) with following steps with **OpenSSL**:

Convert the DER formatted certificate "ewubd SSL cert.cer" to PEM format and save it as "ewubd SSL cert.pem" :

```
C:\OpenSSL\bin>openssl x509 -inform der -in "ewubd SSL cert.cer" -out "ewubd SSL cert.pem"
```

View the certificate: C:\OpenSSL\bin>type "ewubd SSL cert.cer "

Use cat instead of type in Linux systems.

Extract the public key as "ewubd PUB key.key" from the PEM formatted certificate:

```
C:\OpenSSL\bin>openssl x509 -pubkey -in "ewubd SSL cert.pem" -noout > "ewubd PUB key.key"
```

View the public key:

```
C:\OpenSSL\bin>type "ewubd PUB key.key"
```

```
-----BEGIN PUBLIC KEY-----
```

```
MIIBIjANBgkqhkiG9w0BAQEh
```

```
[truncated] QIDAQAB
```

```
-----END PUBLIC KEY-----
```

View the exponent and modulus:

```
C:\OpenSSL\bin>openssl rsa -pubin -in "ewubd PUB key.key" -text -noout
```

```
Public-Key: (2048 bit)
```

```
Modulus:
```

```
00:d2:a5:2c:35:d0:e6:0a:e7:4e:d0:de:83:80:94:
```

```
[truncated]
```

```
b1:85
```

```
Exponent: 8193 (0x10001)
```

</Midterm-1>

<Midterm-2>

Week 5 Homework 17: Practical Cryptography Requirements

Properties of good hash function, encryption and decryption functions.

Strengthening hash functions with Salt

Random and Pseudorandom Number Generation

Week 5 Homework 18: Modern Encryption and Digital Signatures

Message Authentication Code (MAC)

HMAC

DH Key Exchange

RSA Algorithm and $e = 65537$

ECC Algorithm and NISTs 4th EC graph

▶ Elliptic Curve Cryptography Tutorial - Understanding ECC through the Diffie-Hellman Key Excha...

<https://www.youtube.com/watch?v=gAtBM06xwaw>

AES Encryption

3DES Encryption

Known plaintext attack on DES and 2DES algorithms.

▶ The Trick That Solves Rubik's Cubes and Breaks Ciphers (Meet in the Middle)

<https://youtu.be/wL3uWO-KLUE>

SSL Certificates

Kerberos

▶ Taming Kerberos - Computerphile

<https://www.youtube.com/watch?v=qW361k3-BtU>

[Taming Kerberos -- Redmondmag.com](https://redmondmag.com/articles/2004/07/01/taming-kerberos.aspx) [*deep dive into Kerberos*]

<https://redmondmag.com/articles/2004/07/01/taming-kerberos.aspx>

▶ Kerberos Explained (In 3 Levels Of Detail)

<https://www.youtube.com/watch?v=snGeZIDQL2Q>

▶ Basic Kerberos Authentication

<https://www.youtube.com/watch?v=u7MQoSN19O4>

▶ Kerberos Authentication Explained | A deep dive

<https://www.youtube.com/watch?v=5N242XcKAsM>

▶ MicroNugget: How Kerberos Works in Windows Active Directory | CBT Nuggets

<https://www.youtube.com/watch?v=kp5d8Yv3-0c>

[Taming Kerberos – Revx0r](https://revx0r.com/taming-kerberos/)

<https://revx0r.com/taming-kerberos/>

OAuth2 / SAML / Shibboleth SSO

PGP

A Tutorial for Beginners to PGP

<https://sites.pitt.edu/~poole/PGP.htm>

OpenPGP: Key management tool

Email encryption with PGP (Flowcrypt)

VPN (IKE+IPSEC+Tunneling) and TOR

Secure Routing

Wireless Encryption Protocols (WEP, WPA/WPA2/WPA3)

Week 5 and onward: Project: Public Key Infrastructure Implementation

Properties of good hash function, encryption and decryption functions.

Useful tools:

Virtualbox or QEMU or VMWare Player

A Debian based Linux OS

Apache2

OpenSSL

XCA (OpenSSL GUI)

<https://hohnstaedt.de/xca/index.php/download>

Best Practices for Cybersecurity

Effective Cybersecurity by William Stallings

<http://williamstallings.com/Cybersecurity/>

Attack Glossary:

[OWASP Top Ten](#) Vulnerabilities

<https://owasp.org/www-project-top-ten/>

Top 10 Most Common Types of Cyber Attacks

<https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/>

The 15 Most Common Types of Cyber Attacks

<https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/>

1. DDoS

TCP SYN Flood Attack

Teardrop attack

Smurf attack

Ping of death attack

Botnets

Zombie

What is cloudflare?

2. Man-in-the-middle (MitM) attack

Session hijacking

IP Spoofing

Replay

Sniffing

3. Phishing and spear phishing attacks**4. Drive-by attack****5. Password attack**

Brute-force: Crunch, John The Reaper, Hashcat

Dictionary attack: RockYou

Rainbow Table attack

Credential stuffing,

Password spraying

Keylogger

6. SQL injection attack

Buffer Overflow

7. Cross-site scripting (XSS) attack: BeeF XSS Framework**8. Eavesdropping attack: Active or Passive****9. Birthday attack****10. Malware attack**

Macro viruses

File infectors

System or boot-record infectors

Polymorphic viruses

Stealth viruses

Trojans

Logic bombs

Worms

Droppers

Ransomware

Adware

Spyware

Social Engineering Attack

Phishing

Impersonation

Tailgating

Eavesdropping

Shoulder Surfing

Bluetooth Attacks

<https://hackernoon.com/how-to-hack-bluetooth-devices-5-common-vulnerabilities-ng2537af>

Business Email Compromise (BEC)

Phishing

Spear-phishing

Zero-day exploit

Active Persistent Threat

DNS Tunneling

DNS Cache Poisoning

Route poisoning

Cryptojacking

Cookie stealing

AI-Powered Attacks

IoT-Based Attacks

51% attack and other attacks on Blockchains

FAQs:

- What hash format are modern Windows login passwords stored in?
- What are automated tasks called in Linux?
- If a password hash starts with \$6\$, what format is it (Unix variant)?

Threats and Vulnerabilities

- What is the CVE for the 2020 Cross-Site Scripting (XSS) vulnerability found in WPForms?
- There was a Local Privilege Escalation vulnerability found in the Debian version of Apache Tomcat, back in 2016. What's the CVE for this vulnerability?
- What is the very first CVE found in the VLC media player?

- If you wanted to exploit a 2020 buffer overflow in the sudo program, which CVE would you use?

Correct answers are given below, transparency set to 100% to make the picture invisible.



Answer the following questions using the **man** command:

SCP is a tool used to copy files from one computer to another.

What switch would you use to copy an entire directory?

fdisk is a command used to view and alter the partitioning scheme used on your hard drive.

What switch would you use to list the current partitions?

nano is an easy-to-use text editor for Linux. There are arguably better editors (Vim, being the obvious choice); however, nano is a great one to start with.

What switch would you use to make a backup when opening a file with nano?

Netcat is a basic tool used to manually send and receive network requests.

What command would you use to start netcat in listen mode, using port 12345?

Correct answers are given below, transparency set to 100% to make the picture invisible.



Law and Ethics Part

Data Protection

There is a trade-off between Security and Privacy.


Watch the documentary: [The Great Hack](#)

Principles of Data Collection and Use

Resource: Class lecture and SPIC(6) slide in the Resources folder

Regulation of AI

Watch the documentary:

 Artificial intelligence and algorithms: pros and cons | DW Documentary (AI documentary)

<https://youtu.be/s0dMTAQM4cw?t=571>

(Watch from 9:31 to 15:10)

General Data Protection Regulation (GDPR)

How to Comply: GDPR compliance

<https://gdpr.eu/>

Information about GDPR

<https://gdpr-info.eu/>

What is GDPR? The summary guide to GDPR compliance in the UK | WIRED UK

<https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>

General Data Protection Regulation - Wikipedia

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Children's Online Privacy Protection Act (COPPA) (SPIC slide 5)

https://en.wikipedia.org/wiki/Children%27s_Online_Privacy_Protection_Act

The Digital Security Act of 2018 (Bangladesh)

<http://bdlaws.minlaw.gov.bd/act-1261.html>

Official Secrets Act of 1923

<http://bdlaws.minlaw.gov.bd/act-132.html>

</Midterm-2>

<Final>

Bangladesh Data Protection Act 2022

OTT Regulation Act 2022

উপাত্ত সুরক্ষা আইন, ২০২২ (খসড়া) : পর্যালোচনা ও সুপারিশ

[উপাত্ত-সুরক্ষা-আইন-২০২২-এর-খসড়ার-বিষয়ে-জনসাধারণের-মতামত-প্রদানের-লক্ষ্যে-ওয়েবসাইটে](#)

<https://www.facebook.com/TIBangladesh/videos/4568364216597921>

বিস্তারিত জানতে নিচে ক্লিক করুন - <https://www.ti-bangladesh.org/.../6448-2022-05-09-04-33-20>

'উপাত্ত সুরক্ষা আইন' এর খসড়া ঝুঁকিপূর্ণ: টিআইবি

<http://bit.do/fUpnU>

Bangladesh: New data protection bill threatens people's right to privacy - Amnesty International

<https://www.amnesty.org/en/latest/news/2022/04/bangladesh-new-data-protection-bill-threatens-peoples-right-to-privacy/>

“ডিজিটাল-সোশ্যাল-মিডিয়া-এবং-ওটিটি-প্ল্যাটফর্মের-জন্য-বাংলাদেশ-টেলিযোগাযোগ-নিয়ন্ত্রণ

<http://www.btrc.gov.bd/site/notices/2e455d3a-e4d9-421f-94da-0ce0965c3fe0/%E2%80%9C%E0%A6%A1%E0%A6%BF%E0%A6%9C%E0%A6%BF%E0%A6%9F%E0%A6%BE%E0%A6%B2%E0%A6%B8%E0%A7%8B%E0%A6%B6%E0%A7%8D%E0%A6%AF%E0%A6%BE%E0%A6%B2%E0%A6%AE%E0%A6%BF%E0%A6%A1%E0%A6%BF%E0%A6%AF%E0%A6%BC%E0%A6%BE%E0%A6%8F%E0%A6%AC%E0%A6%82%E0%A6%93%E0%A6%9F%E0%A6%BF%E0%A6%9F%E0%A6%BF%E0%A6%AA%E0%A7%8D%E0%A6%B2%E0%A7%8D%E0%A6%AF%E0%A6%BE%E0%A6%9F%E0%A6%AB%E0%A6%B0%E0%A7%8D%E0%A6%AE%E0%A7%87%E0%A6%B0%E0%A6%9C%E0%A6%A8%E0%A7%8D%E0%A6%AF%E0%A6%AC%E0%A6%BE%E0%A6%82%E0%A6%B2%E0%A6%BE%E0%A6%A6%E0%A7%87%E0%A6%B6%E0%A6%9F%E0%A7%87%E0%A6%B2%E0%A6%BF%E0%A6%AF%E0%A7%8B%E0%A6%97%E0%A6%BE%E0%A6%AF%E0%A7%8B%E0%A6%97%E0%A6%A8%E0%A6%BF%E0%A7%9F%E0%A6%A8%E0%A7%8D%E0%A6%A4%E0%A7%8D%E0%A6%B0%E0%A6%A3>

OTT Regulation

[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiGiLSR2vL3AhVjTmwGHRkfCTMQFnoECAYQAQ&url=https%3A%2F%2Fmoi.gov.bd%2Fsites%2Fdefault%2Ffiles%2Ffiles%2Fmoi.portal.gov.bd%2Fnotices%2F164fa44b_7f76_46c9_88a2_ccc4bbbae5f0%2FOtt%2520Nitiba%2520\(Draft\).pdf&usg=AOvVaw04Tc9TBW-Otp6Zy8AoNXec](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiGiLSR2vL3AhVjTmwGHRkfCTMQFnoECAYQAQ&url=https%3A%2F%2Fmoi.gov.bd%2Fsites%2Fdefault%2Ffiles%2Ffiles%2Fmoi.portal.gov.bd%2Fnotices%2F164fa44b_7f76_46c9_88a2_ccc4bbbae5f0%2FOtt%2520Nitiba%2520(Draft).pdf&usg=AOvVaw04Tc9TBW-Otp6Zy8AoNXec)

যা আছে ওটিটি খসড়া নীতিমালায় | প্রথম আলো

<https://www.prothomalo.com/bangladesh/%E0%A6%AF%E0%A6%BE%E0%A6%86%E0%A6%9B%E0%A7%87%E0%A6%93%E0%A6%9F%E0%A6%BF%E0%A6%9F%E0%A6%BF%E0%A6%96%E0%A6%B8%E0%A7%9C%E0%A6%BE%E0%A6%A8%E0%A7%80%E0%A6%A4%E0%A6%BF%E0%A6%AE%E0%A6%BE%E0%A6%B2%E0%A6%BE%E0%A7%9F>

Freedom of expression at Cyberspace

Platform regulation

Community Standards

Whistleblowing and Hacktivism

Digital Governance is a threat?

Surveillance and Censorship in China, North Korea

[Internet censorship - Wikipedia](#)

https://en.wikipedia.org/wiki/Internet_censorship

Digital Divide

Intellectual Property

Every digital copy is of the same quality, while with analog copies qualities degraded

Audio compression: Lossy (mp3) vs. Lossless (FLAC)

Shazam and Google Recognizing Music

 How Shazam Works

<https://www.youtube.com/watch?v=kMNSAhsyiDg>

Lame MP3 encoder

https://en.wikipedia.org/wiki/LAME#Patents_and_legal_issues

Image compression

Video compression

Content distribution Network/Content delivery Network

Client server model versus p2p model

Digital rights management

https://en.wikipedia.org/wiki/Digital_rights_management

Adobe DRM, Widevine CDM/TEE/TPM

<https://pallycon.com/blog/5-things-to-know-about-multi-drm-technology-widevine-part-2/>

Software Protection (Crack keygen KMS etc.)

https://en.wikipedia.org/wiki/Digital_rights_management#Technologies

Intellectual Property Cases

Apple vs. Samsung

Bijoy vs. Avro/Ridmik

Open Source Licenses

Comparison of free and open-source software licenses - Wikipedia

https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses

How to choose a license

<https://choosealicense.com/licenses/>

Open Source Licenses Comparison [Guide]

<https://itsfoss.com/open-source-licenses-explained/>

Cyberethics - Wikipedia

<https://en.wikipedia.org/wiki/Cyberethics>

Computer ethics - Wikipedia

https://en.wikipedia.org/wiki/Computer_ethics

Ethics of artificial intelligence - Wikipedia

https://en.wikipedia.org/wiki/Ethics_of_artificial_intelligence

[Do not cite Wikipedia, rather use the cited materials in the Wikipedia article, instead.]

Ethical Theories

SPIC (17) and SPIC (18)

SPIC Lectures

<https://drive.google.com/drive/folders/1C9MnLCrOXLbcwGGoMWGetGclrV7za9rh?usp=sharing>

Aristotelian Ethics: Virtue Ethics

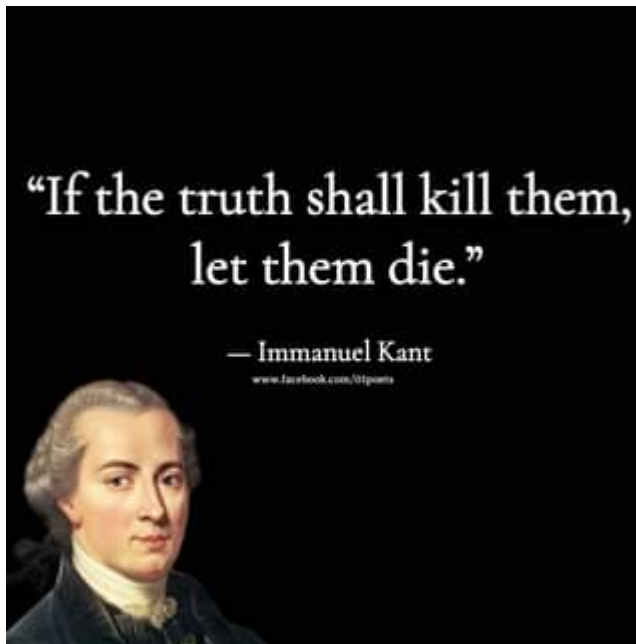
▶ Aristotle & Virtue Theory: Crash Course Philosophy #38

<https://www.youtube.com/watch?v=PrvtOWEXDIQ>

Deontological Ethical Theories (Duty-based, not morality-based)

From Wikipedia: In [moral philosophy](#), **deontological ethics** or **deontology** (from [Greek](#): δέον, 'obligation, duty' + λόγος, 'study') is the [normative ethical](#) theory that the [morality](#) of an action should be based on whether that action itself is right or wrong under a series of rules, rather than based on the consequences of the action. It is sometimes described as [duty-](#), [obligation-](#), or rule-based ethics.

Deontological ethics is commonly contrasted to [consequentialism](#), [virtue ethics](#), and [pragmatic ethics](#). In this [terminology](#), action is more important than the consequences.

**(Absolutism) The view of Immanuel Kant**

▶ Kant & Categorical Imperatives: Crash Course Philosophy #35

<https://www.youtube.com/watch?v=8blys6JoEDw>

Consequentialist Ethical Theories

Consequentialism is a class of [normative](#), teleological [ethical theories](#) that holds that the [consequences](#) of one's conduct are the ultimate basis for judgment about the rightness or wrongness of that conduct. Thus, from a consequentialist standpoint, a morally right act (or omission from acting) is one that will produce a good outcome. Consequentialism, along with [eudaimonism](#), falls under the broader category of **teleological ethics**, a group of views which claim that the moral value of any act consists in its tendency to produce things of [intrinsic value](#). Consequentialists hold in general that an act is right *if and only if* the act (or in some views, the rule under which it falls) will produce, will probably produce, or is intended to produce, a greater balance of good over evil than any available alternative. Different consequentialist theories differ in how they define [moral goods](#), with chief candidates including pleasure, the absence of pain, the satisfaction of one's preferences, and broader notions of the "general good".

(Uti-lita-ria-nism) The view of John Stuart Mill

▶ Utilitarianism: Crash Course Philosophy #36

<https://www.youtube.com/watch?v=-a739VjqdSI>

▶ Utilitarianism | Ethics Defined

https://www.youtube.com/watch?v=-FrZI22_79Q

▶ Utilitarianism in 4 Minutes

<https://www.youtube.com/watch?v=mL7Pt-NHraU>

▶ Utilitarianism - John Stuart Mill

<https://www.youtube.com/watch?v=Dr9954kaFBs>

▶ PHILOSOPHY - Ethics: Utilitarianism, Part 1 [HD]

<https://www.youtube.com/watch?v=uvmz5E75ZIA>

▶ PHILOSOPHY - Ethics: Utilitarianism, Part 2 [HD]

<https://www.youtube.com/watch?v=uGDk23Q0S9E>

▶ PHILOSOPHY - Ethics: Utilitarianism, Part 3 [HD]

<https://www.youtube.com/watch?v=MoCuVa9UeR4>

John Rawls' Theory of Justice

■ Rawls Theory of Justice Summary .pdf

<https://drive.google.com/file/d/1CzND9pflcED4yL63RRMYrAJ5KuGX3AiM/view?usp=sharing>

A Theory of Justice Study Guide

<https://www.enotes.com/topics/theory-justice>

▶ What Is Justice?: Crash Course Philosophy #40

<https://www.youtube.com/watch?v=H0CTHVCKm90>

Professional Ethics and Responsibilities for Computer Scientists and Engineers

[Chapter 9 of the Sara Baase Book]

A.1. Software Engineering Code of Ethics and Professional Practice

[Software Engineering Code - ACM Ethics](#)

<https://ethics.acm.org/code-of-ethics/software-engineering-code/>

A.2. ACM Code of Ethics and Professional Conduct

[ACM Code of Ethics and Professional Conduct](#)

<https://www.acm.org/code-of-ethics>

The System Administrators' Code of Ethics

<https://lopsa.org/CodeofEthics>

SE Code of Ethics | CS 3240 - F20

<http://cs3240.cs.virginia.edu/f20/lecture/ethics/2020/09/16/secode.html>

Computer Ethics | Ethics, Laws, Definition & Privacy

<https://teachcomputerscience.com/computer-ethics/>

IEEE CODE OF CONDUCT

https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/ieee_code_of_conduct.pdf

IEEE Code of Ethics

<https://www.ieee.org/about/corporate/governance/p7-8.html>

**Ethical Decision Making in the field of IT and Computer Science:
Case studies, Group debate and Report Writing****Thinking Ethically - Markkula Center for Applied Ethics**

<https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/thinking-ethically/>

A Framework for Ethical Decision Making

<https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making/>

An Introduction to Cybersecurity Ethics

<https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf>

Steps to Ethical Decision Making (by Sara Baase):

Textbook: S. Baase, *A Gift of Fire: Social, Legal, And Ethical Issues For Computing Technology* (4th edition), Boston, MA, United States: Prentice Hall, 2012.

Reference:

A. Adams and R. J. McCrindle, *Pandora's box: Social and professional issues of the information age*. Chichester, England: Wiley, John & Sons, 2008.

J. M. Kizza, *Ethical and social issues in the information age*, 5th ed. London: Springer-Verlag New York, 2013.

Brainstorming phase:

- List all the people and organizations affected. (They are the stakeholders.)
- List risks, issues, problems, consequences.
- List benefits. Identify who gets each benefit.
- In cases where there is not a simple yes or no decision, but rather one has to choose some action, list possible actions.

Analysis phase:

- Identify responsibilities of the decision maker. (Consider responsibilities of both general ethics and professional ethics, as per **ACM/SE Codes of Ethics**.)
- Identify the rights of stakeholders. (It might be helpful to clarify whether they are negative or positive rights)
- Consider the impact of the action options on the stakeholders.
- Analyze consequences, risks, benefits, harms, and costs for each action considered.
- Consider Kant's, Mill's, and Rawls' approaches.
- Then, categorize each potential action or response as ethically obligatory, ethically prohibited, or ethically acceptable.

Decision Phase:

If there are several ethically acceptable options, select an option by considering the ethical merits of each, courtesy to others, practicality, self-interest, personal preferences, and so on. (In such a case, plan a sequence of actions, depending on the response to each.)

Mini Project-3: Present an ethical dilemma in decision making in the field of IT.

Activity: Criticism and justification of actions/stance as per ethical frameworks

Case studies with **group presentation and opposition**

Own report writing and Opposition report writing

The Report should contain (Limit 4 pages)

- ☐ Details of a case/scenario that involves an ethical dilemma and requires decision making in an ethical manner
- ☐ Identify the dilemma clearly and the possible/probable decisions
- ☐ Justification of the chosen decision based on the Ethical Theories following the steps to ethical decision making.
 - ☐ Brainstorming Phase
 - ☐ Analysis Phase
 - ☐ Decision Phase

Topics could be:

- Self-driving cars (The Moral Machine)
- Use of machine learning for adversarial purpose (Uyghur Detection Dataset)
- Social Rating System
- Limits to Ethical Hacking
- Trustworthiness of AI
 - [Trustworthy AI and the foundations of AI systems - Ericsson](#)
 - [AI – Ethics inside? - Ericsson](#)
 - [AI bias and human rights: Why ethical AI matters - Ericsson](#)
 - [Trustworthy AI | IBM](#)
 - [AI Ethics | IBM](#)
 - [Ethics guidelines for trustworthy AI | Shaping Europe's digital future](#)
- More topics could be found in: [Ethics of artificial intelligence - Wikipedia](#)
- Chapter 9 of the Book: A Gift of Fire by Sara Baase.

Resources:**Links:**

[Moral Machine](#)
[The Moral Machine experiment | Nature](#)
[Moral Machine - Wikipedia](#)
[Why the moral machine is a monster](#) [PDF]

TED talks:

The ethical dilemma of self-driving cars - Patrick Lin
<https://www.youtube.com/watch?v=ixloDYVfKA0>
The Social Dilemma of Driverless Cars - Iyad Rahwan
<https://www.youtube.com/watch?v=nhCh1pBsS80>
The Greater Good - Mind Field S2 (Ep 1: The Trolley Problem in Real life)
<https://www.youtube.com/watch?v=1sl5KJ69qiA>

The following will be the drill for debate session:

- *The defending group will have 6 minutes to complete their presentation.*
- *Then the opponent group will have 3 minutes to present the opposition, and keep the screen on until the end of the session.*
- *Then the defending group will have 1 minute to present for the rebuttal.*
- *Open discussion/debate on the decision will follow for 2 minutes.*

The following will be the drill for debate session:

- *The defending group will have 6 minutes to complete their presentation.*
- *Then the opponent group will have 3 minutes to present the opposition, and keep the screen on until the end of the session.*
- *Then the defending group will have 1 minute to present for the rebuttal.*
- *Open discussion/debate on the decision will follow for 2 minutes.*

The **Defending group** shall present their work for 6 minutes. This could be 3 x 2 minute presentations, or the group leader may present the whole presentation.

The defense presentation (6 minutes) and the report (limit: 4 pages) should highlight:

- ☐ The presented scenario and the probable decisions
- ☐ The ethical dilemma associated with each of the decisions
- ☐ Analysis of each of the decisions showing every steps of the decision making process (both brainstorming and analysis phase) [**should be emphasized**]
- ☐ Responsibility of you as a decision maker and the rights of the stakeholders
- ☐ Justification of the chosen decision based on the ethical theories [***most emphasis should be given***]

The opposition report should be submitted before 23:55

The opposition report (limit: 2 pages) and presentation (3 minutes) should highlight

- ☐ Summary of the opponents' scenario and ethical dilemma
- ☐ Strongest aspect of the opponents' work
- ☐ Weakest aspect of the opponents' work
- ☐ Suggestions/Criticisms to the opponents' decision [***most emphasis should be given***]

The defending group shall refute the opponents' criticisms for 1 minute, followed by an open discussion/debate session for 2 minutes.

Marks distribution of the MP-3 will be as follows:

| Activity | Mark |
|----------------|------|
| Project Report | 5 |

| | |
|--------------------------|----|
| Defense Presentation | 2 |
| Opposition Report | 3 |
| Opposition Presentation | 3 |
| Rebuttal/Open Discussion | 2 |
| Total | 15 |

<Final>

Knowledgebase

Hash Functions