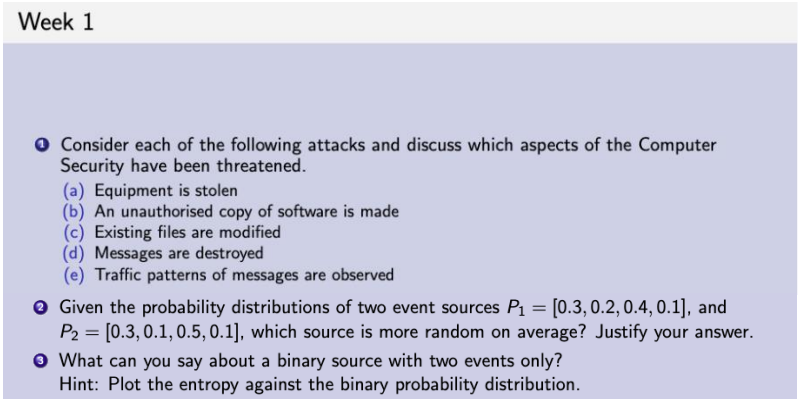
Name: Thomas McAloon
Student Reference: 33618177



Week 1

1. Consider each of the following attacks and discuss which aspects of the Computer Security have been threatened.
   (a) Equipment is stolen
   (b) An unauthorised copy of software is made
   (c) Existing files are modified
   (d) Messages are destroyed
   (e) Traffic patterns of messages are observed
2. Given the probability distributions of two event sources $P_1 = [0.3, 0.2, 0.4, 0.1]$, and $P_2 = [0.3, 0.1, 0.5, 0.1]$, which source is more random on average? Justify your answer.
3. What can you say about a binary source with two events only?
   Hint: Plot the entropy against the binary probability distribution.

1.

a. Equipment is stolen:

Physical theft of computer equipment poses a threat to the security of an organization's assets. The loss of laptops, desktops, servers, or other electronic devices can result in unauthorized access to sensitive information, data loss, and system downtime. Furthermore, replacement of the stolen equipment can cause financial loss. This type of attack primarily affects physical security, access control, and data confidentiality.

A senior hospital manager at Colchester University Hospital NHS Foundation Trust was suspended after his unencrypted laptop was stolen from his car in Edinburgh, Scotland. The laptop contained the unencrypted records of over 20,000 patients, including patient names, postcodes, and treatment plans.
Source: https://www.digitalhealth.net/2008/07/nhs-manager-suspended-after-losing-laptop/

b. An unauthorized copy of software is made:

Unauthorized copying of software is a violation of licensing agreements and poses legal and financial risks for both the individual and the organization. This attack can also expose systems to malware and other cyber threats, compromising the security of the system. This type of attack primarily affects software security, access control, and legal compliance.

In 2017, the ransomware WannaCry spread across the world, infecting more than 200,000 computers in 150 countries. It exploited a vulnerability in Windows that had been identified by the US National Security Agency and leaked online. The ransomware demanded payment in Bitcoin to unlock encrypted files. Many of the affected systems were running unlicensed or unsupported software, making them more vulnerable to the attack.
Source: https://www.bbc.com/news/technology-40416611

c. Existing files are modified:

Unauthorized modification of files on a system can corrupt data, cause data loss, and expose sensitive information to unauthorized access. This type of attack primarily affects data integrity, access control, and data confidentiality.

In 2020, Hackney Council in London suffered a cyber-attack that disrupted its services for several weeks. The attackers gained access to the council's IT systems and encrypted files, demanding payment in exchange for the decryption key. The

council refused to pay and was able to restore its systems from backups, but some data was lost. The attack was described as "sophisticated and malicious".
Source: https://www.wired.co.uk/article/ransomware-attack-recovery-hackney

d. **Messages are destroyed:**
Destruction of messages or information on a system can result in loss of critical data, communication breakdowns, and unauthorized access to sensitive information. This type of attack primarily affects system availability, data integrity, and data confidentiality.

In 2021, a ransomware attack on the Irish health service led to the disruption of its systems, including the shutdown of its email and IT systems. The attackers demanded a ransom to restore the encrypted data. The Irish government refused to pay and instead worked to restore its systems, which took several weeks. The attack was described as the most significant cyber-attack on the Irish state.
Source: https://www.theguardian.com/world/2021/may/14/ransomware-attack-disrupts-irish-health-services

e. **Traffic patterns of messages are observed:**
Observation of network traffic patterns can reveal communication patterns, sources and destinations of messages, and other sensitive information. This can lead to unauthorized access to sensitive data and communication breakdowns. This type of attack primarily affects data confidentiality, data integrity, and access control.

In 2021, it was reported that the Chinese government had been using fake LinkedIn profiles to spy on and gather information about politicians, government officials, and military personnel in Europe and other countries. The profiles would send messages containing malicious links or attachments, which would then be used to gain access to sensitive information. The attack was described as "a very effective and low-cost way of getting access to senior political figures".
Source: https://www.bbc.co.uk/news/technology-56812746

2. To determine which source is more random on average, we can calculate the entropy of each source and compare the results.
The entropy of a discrete probability distribution is given by the formula:

- $H = - \Sigma (p(i) * \log2(p(i)))$
- $p(i)$ is the probability of the ith event in the distribution.

For source P1, we have:

- $H(P1) = - (0.3 * \log2(0.3) + 0.2 * \log2(0.2) + 0.4 * \log2(0.4) + 0.1 * \log2(0.1)) = 1.8464$ bits/event

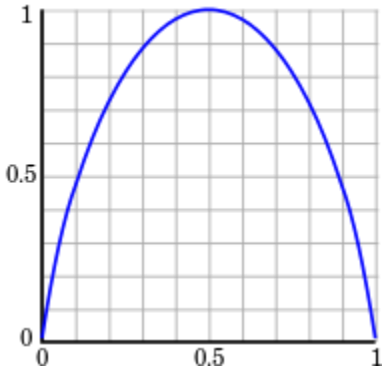
For source P2, we have:

- $H(P2) = - (0.3 * \log2(0.3) + 0.1 * \log2(0.1) + 0.5 * \log2(0.5) + 0.1 * \log2(0.1)) = 1.8464$ bits/event

Therefore, both sources have the same entropy, which is 1.8464 bits/event indicating that both sources have the same amount of randomness on average.

3. A binary source is a source of data that can only produce one of two possible outcomes. For example, a coin toss can result in either heads or tails, making it a binary source. The entropy of a binary source is a measure of how much uncertainty or randomness is present in the source.

   Entropy can be plotted against the probability distribution of the two possible outcomes. When both outcomes are equally likely (probability of 0.5), the entropy is at its maximum value, meaning the source is maximally uncertain or random. As one outcome becomes more likely than the other, the entropy decreases and reaches a minimum value of 0 when one outcome is certain to occur.



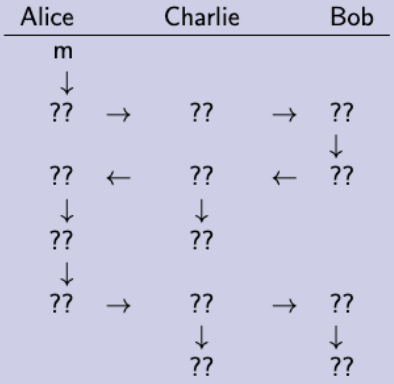
   Therefore, the entropy of a binary source provides a way to quantify the randomness or uncertainty of the source. It is maximized when both outcomes are equally likely and decreases as one outcome becomes more likely than the other. This concept is useful in information theory and has many practical applications in cryptography, coding theory, and data compression.

Name: Thomas McAloon
Student Reference: 33618177

Week 2

John proposes a cryptosystem that is based on one-time key pad and requires no key exchange. It works as follows: If she wants to send Bob a message m, Alice generates her key k_a, a sequence of random bits (the same length as m), computes $c = m \oplus k_a$ and sends c to Bob, where $\oplus$ represents the bitwise XOR operation. On receipt of c, Bob generates his own random bits k_b of same length, computes $d = c \oplus k_b$ and sends d to Alice. On receipt of d, Alice computes $e = d \oplus k_a$ and sends e to Bob. On receipt of e, Bob computes $e \oplus k_b$ for the last time.
Analyse John's cryptosystem and conclude whether John's cryptosystem works.

The following format may be adopted to help demonstrate what happens with the plaintext m that from Alice to Bob, where "??" parts are for you to figure out. Each of the 3 columns shows the series of the values (or texts) visible by Alice, Bob or Charlie.



John's proposed cryptosystem is a variation of the one-time pad (OTP) cipher, which is theoretically unbreakable if used correctly. OTP works by generating a random key of the same length as the plaintext message, and XORing the key with the message to produce the ciphertext. The same key is used to decrypt the ciphertext to produce the original message.

In John's proposed cryptosystem, Alice generates her key k_a, XORs it with the plaintext message m to produce the ciphertext c, and sends it to Bob. Bob generates his own random key k_b, XORs it with the ciphertext c to produce d, and sends it back to Alice. Alice XORs d with her own key ka to produce e, which she sends back to Bob. Finally, Bob XORs e with his own key kb to recover the original plaintext message m.

The security of John's cryptosystem relies on the randomness of the keys k_a and k_b. If these keys are truly random and used only once, then the ciphertext will be indistinguishable from random noise, making it difficult for an attacker to determine the plaintext message.

However, John's cryptosystem has some major weaknesses:

- First, the keys ka and kb must be truly random and used only once. If either key is not random or is reused, an attacker can easily recover the plaintext message.

- Second, John's cryptosystem is vulnerable to a known plaintext attack, where an attacker who knows some plaintext and corresponding ciphertext can easily recover the keys k_a and k_b.
- Third, John's cryptosystem requires two rounds of communication between Alice and Bob, making it slower and less efficient than other cryptosystems that only require one round of communication.

In conclusion, John's cryptosystem is not secure enough for practical use as it has major weaknesses that make it vulnerable to attacks. It is based on the theoretically unbreakable OTP cipher, but the use of non-random or reused keys, vulnerability to known plaintext attacks, and inefficiency make it impractical for secure communication.

Alice's View	Charlie's View	Bob's View
m	-	-
↓		↓
ka	-	-
↓		↓
c = m ⊕ ka	-	-
	↓	kb
		↓
d = c ⊕ kb	-	-
↓		↓
e = d ⊕ ka	-	-
↓		-
-	e	-
↓		-
-	e ⊕ kb	-

Week 3

❷ Let the password seed be 1101 which is known by both Alice and Bob.
(a) Demonstrate how Alice and Bob can independently generate an identical new random password of up to 15 bits without sending the new password.
(b) What are the risks?

(a) Alice and Bob can use the password seed 1101 to generate new random passwords of up to 15 bits without exchanging the new password by utilising the Caesar cipher algorithm. The Caesar cipher is a substitution cipher that replaces each letter in the plaintext by a letter a fixed number of positions down the alphabet. In this case, the Caesar cipher will be used to encrypt the password seed with a randomly generated number of shifts (i.e., the key), which will result in the generation of a new password. Since the password seed is known by both Alice and Bob, they can independently generate the same new password without communicating it over an insecure channel.

To generate the new password, Alice and Bob can perform the following steps:

1. Generate a random number n between 1 and 25 to use as the key for the Caesar cipher.
2. Alice and Bob each independently encrypt the password seed with the key n using the Caesar cipher algorithm.
3. Alice and Bob each independently obtain the resulting ciphertext from the encryption process.
4. Alice and Bob each store the ciphertext as their new password.

Since both Alice and Bob have used the same password seed and key value, they will each generate the same new password.

(b) There are several risks associated with using the Caesar cipher with a fixed password seed and a randomly generated key to generate new passwords:

1. Lack of confidentiality: Although Alice and Bob can generate new passwords without communicating them over an insecure channel, the passwords are not confidential since they can be easily decrypted by an attacker who intercepts the ciphertext and knows the Caesar cipher algorithm and the key value.

2. Weak encryption: The Caesar cipher is a relatively weak encryption algorithm since it only uses a simple substitution technique. This makes it vulnerable to attacks such as frequency analysis, where an attacker can analyze the frequency of letters in the ciphertext and use this information to deduce the key value and recover the original plaintext.

3. Key reuse: If the same key value is used for multiple passwords, an attacker can use frequency analysis to break the encryption and recover the original plaintext. This is because the same letters will be encrypted with the same key value and will produce the same ciphertext.

4. Lack of authentication: The Caesar cipher does not provide any authentication mechanism, which means that an attacker can modify the ciphertext without being detected. This can result in unauthorized access to sensitive data.

Overall, the use of the Caesar cipher with a fixed password seed and a randomly generated key presents several security risks, and it is recommended to use a stronger encryption algorithm and a unique key value for each password generated. Additionally, other security measures such as authentication and access control should also be implemented to provide better protection for sensitive data.

Week 4

- Demonstrate how the Vernam cipher works for the example of plaintext "computer" and the one-time pad (5 20 0 9 17 16 22 18). Explain why the cipher is hopeless in practice.
- Explain how the transposition cipher works. Demonstrate how the plaintext can be decrypted from the ciphertext HKFPRZNIWUVLG UOJOEO TCNMEAOEBOETYCQRXDHDE, using the key IAMTHE.
- Consider the RSA (Rivest, Shamir and Adleman) cryptosystem. Before sending a message $m = 3$ to Alice, Bob prepares his keys carefully. He randomly chooses $p = 5$, $q = 7$ and $e = 7$. Answer the following questions on the RSA cryptosystem. Show all your work.
  - (a) What is the value of n, the RSA modulus?
  - (b) What is the value of $r = \varphi(n)$?
  - (c) What is the value of the decryption exponent d?
  - (d) Which values are used as Bob's *private key*?
  - (e) Which values are used as Bob's *public key*?

4. The Vernam cipher, also known as the one-time pad, is a symmetric encryption algorithm that uses a random key that is at least as long as the plaintext. The key is added modulo 26 to the plaintext to produce the ciphertext, and the same key is used by the recipient to decrypt the message.

Plain Text	**C**	**O**	**M**	**P**	**U**	**T**	**E**	**R**
Key	5	20	0	9	17	16	22	18
Cipher Text	J	X	M	Y	B	K	W	K

To encrypt the first letter, "c" (which corresponds to the third letter in the alphabet), we add the first number in the key, 5 (which corresponds to the sixth letter in the alphabet), modulo 26: (3 + 5) mod 26 = 8, which corresponds to the letter "i". Continuing in this way, we get the ciphertext "jxmybkwk".

The Vernam cipher is theoretically unbreakable, as long as the key is truly random, used only once, and kept secret from everyone except the sender and receiver. However, in practice, it is almost impossible to generate truly random keys, and any deviation from perfect randomness in the key can lead to vulnerabilities that can be exploited by an attacker. Additionally, the key must be securely transmitted between the sender and receiver, which can be a challenge. Finally, the key can only be used once, which means that the sender and receiver must have a way to generate new, random keys for each message. All of these factors make the Vernam cipher impractical for most real-world applications.

- Explain how the transposition cipher works. Demonstrate how the plaintext can be decrypted from the ciphertext HKFPRZNIWUVLG UOJOEO TCNMEAOEBOETYCQRXDHDE, using the key IAMTHE.

5. The transposition cipher works by rearranging the order of the letters in the plaintext.

   Decryption of a transposition cipher is done by:
   - Knowing the key
   - Numbering the key in alphabetic order
   - Number of Lines = Length(message)/Length(Key)
   - Input the message by columns in alphabetic order

The plaintext before Decryption: HKFPRZNIWUVLGUOJOEOTCNMEAOEBOETYCQRXDHDE

First, we'd have to write out the key in a row with all the letters. The order of the letters in the row should be the same as the order of the letters in the key. Then, we'd write the plaintext in groups of 5 letters underneath the row, so that each group of 5 letters is directly underneath one of the letters in the row.

A	E	H	I	M	T
1	**2**	**3**	**4**	**5**	**6**
H	I	U	T	E	Q
K	W	O	C	B	R
F	U	J	N	O	X
P	V	O	M	E	D
R	L	E	E	T	H
Z	G	O	A	Y	D
N	-	-	O	C	E

The final step is to rearrange the letters in each block to match the order of the letters in the key.

I	A	M	T	H	E
4	**1**	**5**	**6**	**3**	**2**
T	H	E	Q	U	I
C	K	B	R	O	W
N	F	O	X	J	U
M	P	E	D	O	V
E	R	T	H	E	L
A	Z	Y	D	O	G
O	N	C	E	-	-

The plaintext after Decryption is THEQUICKBROWNFOXJUMPEDOVERTHELAZYDOGONCE.

6. Consider the RSA (Rivest, Shamir and Adleman) cryptosystem. Before sending a message $m = 3$ to Alice, Bob prepares his keys carefully. He randomly chooses $p = 5$, $q = 7$ and $e = 7$. Answer the following questions on the RSA cryptosystem. Show all your work.
   (a) What is the value of n, the RSA modulus?
   (b) What is the value of $r = \varphi(n)$?
   (c) What is the value of the decryption exponent d?
   (d) Which values are used as Bob's *private key*?
   (e) Which values are used as Bob's *public key*?

6.

(a) Calculate the value of n, the RSA modulus:

- n = p * q
- n = 5 * 7
- n = 35

(b) Calculate the value of r = '(n):

- r = (p - 1) * (q - 1)
- r = (5 - 1) * (7 - 1)
- r = 24

(c) To find the value of the decryption exponent d, we use the formula:

- d x e ≡ 1 (mod r)
- d x 7 ≡ 1 (mod 24)

Euclidean algorithm:

- 24 = 3 x 7 + 3
- 7 = 2 x 3 + 1

Substituting back:

- 1 = 7 - 2 x 3
- = 7 - 2 × (24 - 3 × 7)
- = 7 × 7 - 2 × 24
- d × 7 ≡ 1 (mod 24)
- Therefore, d = 7.

(d) d Bob's private key consists of the values p, q, and d:

- p = 5
- q = 7
- d = 7

(e) Bob's public key consists of the values n and e:

- n = 35
- e = 7
- Public Key = {35, 7}

Name: Thomas McAloon
Student Reference: 33618177

Week 5

If g is a generator for prime p, then the value of $g^n \mod p$ is a different value for every $n \in [1, p-1]$.

1. Show $g = 3$ is a generator for $p = 17$.
2. Show $g = 2$ is not a generator for $p = 17$.

[Hints]

n	1	2	$\cdots$	$p-1$
$g^n \mod p$			$\cdots$	

1. To show that g = 3 is a generator for p = 17, we must work out each integer in the range [1, 16] by taking 3 raised to some power modulo 17.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
g^n mod p	3	9	10	13	5	15	11	16	14	4	12	2	6	8	7	1

Since every integer in the range [1, 16] can be obtained by taking 3 raised to some power modulo 17, we can conclude that g = 3 is a generator for p = 17.

2. To show that g = 2 is not a generator for p = 17, at least one integer in the range [1, 16] cannot be obtained by taking 2 raised to some power modulo 17.

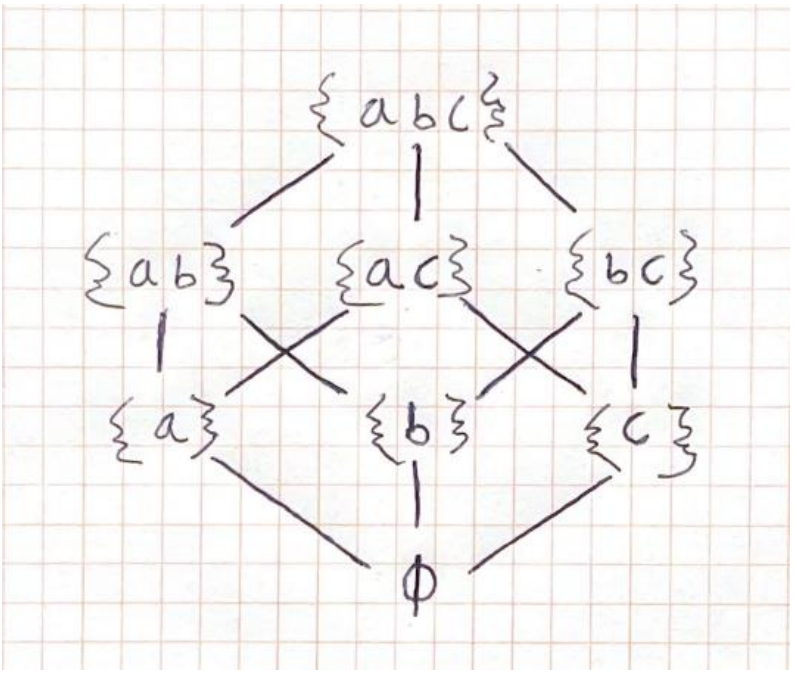
n	1	2	3	4	5	6	7	8
g^n mod p	2	4	8	16	13	9	1	2

We see that 2^8 mod 17 = 2, which means that 2 is not a generator for p = 17, since we have a repeated value (2) before we can obtain all integers in the range [1, 16].

Week 7

Let L be the *power set* of (a,b,c). The system low is $\emptyset$ and the system high is (a, b, c). Draw the lattice for $(L, \subset)$.

L = Power set of {a,b,c} = { ∅, {a}, {b}, {c}, {a,b}, {a,c}, {b,c}, {a,b,c} }



Here, each node represents an element of the power set, and edges connect elements that are immediate subsets of each other. The lowest element is represented by ∅ at the bottom, and the highest element is represented by {a,b,c} at the top.

Week 8

Discuss the sensitivity of each of the following disclosures and explain why.

i. The sum of all financial supports for students in our department.
ii. A list of students receiving financial supports in our department.
iii. Charlie got the above sum in January and the list in October.
iv. What computation would a database management system have to perform in order to determine that the list of names might reveal sensitive data?

The sensitivity of data disclosures can vary greatly depending on the context in which they are made. In the case of financial support for students in a department, both the total sum of support and the list of students receiving support can be sensitive information.

Firstly, the total sum of financial support can reveal information about the department's budget, allocation of resources, and priorities. This information can potentially be used by

competitors or other parties to make strategic decisions or gain an advantage over the department.

Secondly, the list of students receiving financial support can reveal personal information about those individuals, such as their financial situation, academic performance, or other personal circumstances. This information can be sensitive and private, and the disclosure of such information can violate the privacy and confidentiality of the individuals involved.

Furthermore, the timing of disclosures can also impact their sensitivity. In the case of Charlie receiving the sum in January and the list in October, the disclosure of the list of students receiving support after Charlie received the sum can potentially reveal that Charlie received support. This can potentially be sensitive information and impact the privacy and confidentiality of Charlie's financial situation.

In terms of database management, a system would have to perform computations to analyse the data and identify potentially sensitive information. This could involve identifying patterns or relationships between data points, flagging data points that meet certain criteria, or applying machine learning algorithms to predict sensitive information based on past data. However, it is important to note that such analysis should be done with appropriate privacy and security measures in place to protect the confidentiality of the individuals involved.