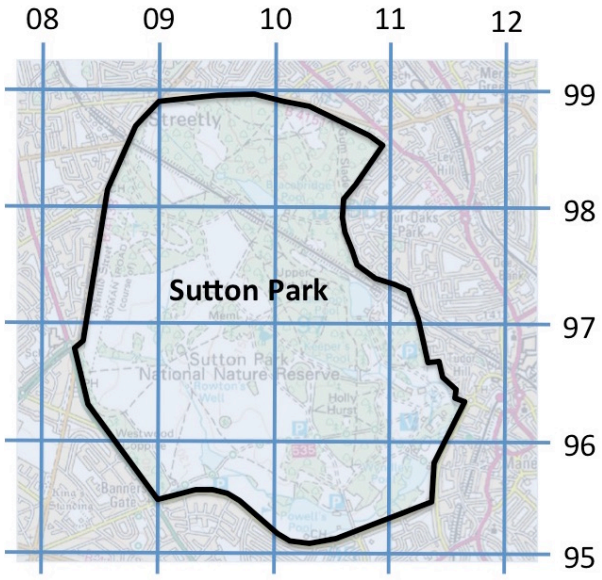
1. To answer this question about **cryptanalysis**, you need to know that an Ordnance Survey (OS) grid reference is a 10-digit number that precisely locates a point on a map. It is actually made up of two 5-digit numbers; the first is the easting and the second is the northing. The OS divides the UK up into a grid of 1-kilometre squares. On the map of *Sutton Park* below, each vertical grid line is numbered and this represents the 1st 2 digits of the easting. Similarly, each horizontal grid line is numbered, representing the 1st 2 digits of the northing. For example, in the map, the word "Sutton" is contained within the 1km square denoted by the grid reference 09---97---, and the centre of the first 'o' in "Sutton" is located at 0970097280, where 09700 is the easting and 97280 is the northing.



a) Robby Banks, a habitual criminal, is arrested at Birmingham Airport on suspicion of committing a bank robbery. When arrested, he is found to have the following letter in his position, which he was about to post to "Shifty" Jim Magee, a shady solicitor.

> Dear Shifty,
>
> The cops are on my tail so I'm simply going to shift my location for a few months until they are off the scent. In the meantime, I simply want you to shift the takings from my last bank job from where they are buried and use them to buy the NIGHTSHIFT'S ARMS pub to set me up for my retirement (simply shift your usual fee into your account). The cash is buried at 7669064042.
>
> ~~IF YOU TELL THE COPS YOU'LL BE SORRY!!~~
> Regards to Sally and the kids,
>
> Robby

PC Yasmin Khan, investigating officer for the case, recognizes **7669064042** as a grid reference, but when she looks it up on a map it turns out to be a point out in the sea. She therefore concludes that 7669064042 is **ciphertext** and something in the letter leads PC Khan to think that Banks has used a simple **shift cypher** to **encrypt** the true grid reference using a key **k** known only to himself and Magee. Banks refuses to reveal the key and Magee is nowhere to be found. However, Banks' getaway car is discovered abandoned in Sutton

Park with a spade in the boot, and PC Khan suspects that the money is buried somewhere in the park.

i. Given that a grid reference is a set of ten decimal digits, how many possible values of **k** are there likely to be, and what values could **k** have?

(2 marks)

ii. Help PC Khan find the buried money by inferring **k** and using it to **decrypt** the grid reference. Be careful to explain your reasoning and show your working.

(15 marks)

iii. If PC Khan had not had her insight that the money was likely to be buried in Sutton Park, what would have been the effect on the recovery of the stolen money by the police? Justify your answer.

(2 marks)

b) Now imagine that in 5 year's time Banks is released from prison but falls back into old habits. He robs another bank and buries the money. He uses a simple **shift cypher** again, but under the impression that it will give him better security, he uses a larger **alphabet** for the value of **k** as follows (showing the ordinal value for each character):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

0	1	2	3	4	5	6	7	8	9
26	27	28	29	30	31	32	33	34	35

i. Banks chooses **k = 24**. Use it to encrypt the grid reference of the burial location

1032498107

(4 marks)

ii. The newly promoted Detective Sergeant Khan again recognizes that the **ciphertext** is a grid reference but must identify the alphabet used for k before she can infer **k** itself. Are there any clues in the **ciphertext** you derived in part (i) that could lead DS Khan to identify the alphabet and the likely range of values for **k**?

(2 marks)

2. A small art gallery's most valuable artwork is protected by an **Internet-enabled smart video camera** in the part of the gallery in which the artwork is situated. An app on the gallery curator's smartphone allows her to stream the camera's video in real time. When the camera's image processing software detects motion in the room, the camera **publishes** an **event** on the art gallery's network. Two software agents **subscribe** to this event. The first agent generates an alert on the gallery curator's **smartphone**. The second agent archives the generated video in a **time-stamped file** on a **cloud server**, stopping whenever no motion has been detected for 5 seconds. Archived video is deleted from the cloud server when it is one month old.

   a) Identify one **hardware**, one **software** and one **data** asset.

   (3 marks)

   b) Identify three **vulnerabilities**.

   (6 marks)

   c) Identify one **threat** for each of **confidentiality**, **integrity** and **availability**.

   (6 marks)

   d) The primary threat is to **confidentiality**. Do you agree with this statement? Justify your answer.

   (4 marks)

   e) Briefly describe suitable **controls** for three **threats** you identified in (c).

   (6 marks)

3. Alice is a senior politician. Bob is a government lawyer. Communication between Alice and Bob takes place over the Internet but using the government's closed-domain public key infrastructure (**PKI**) to ensure that communications can be trusted. Assume that the root Certification Authority (**CA**) is trusted. Alice wants to get Bob's legal advice about a piece of sensitive legislation that she is writing.

   a) Alice **encrypts** the document containing the draft legislation using Bob's **public key**. Which of the three goals of information security should this achieve and how?

   (2 marks)

   b) Alice obtains Bob's public key from the **X.509 digital certificate** issued to Bob by the root CA. Besides Bob's public key, identify two other important items of information contained in the certificate.

   (2 marks)

   c) Explain how:

      i. Alice can verify that the certificate's **integrity** has not been compromised by (e.g.) an attacker modifying the certificate.

      (2 marks)

      ii. Alice can verify that the certificate has been issued by the **root CA**.

      (2 marks)

      iii. Alice can **authenticate** Bob.

      (1 mark)

   d) Now that Bob has been **authenticated** and the certificate's integrity verified, is it safe for Alice to **encrypt** the document with the **public key** it contains and send it to Bob? Explain your answer.

   (3 marks)

   e) Alice often asks Bob for advice. If the advice is to do something Alice finds inconvenient, she frequently ignores it, and when challenged by other politicians, denies that advice was ever sought. Bob is fed up of being used like this. He refuses to accept the document until Alice takes some additional action so that she cannot **repudiate** her request. What is this action called, how can Alice achieve it, and how can Bob use it prove that Alice sent the document?

   (3 marks)

   f) Root CAs are sometimes termed **trusted third parties**. What does this mean and what kind of event could cause Alice or Bob to lose trust in the **CA**?

   (3 marks)

   g) A **hash function** for A is a function $h : A \rightarrow B$

      i. State one general property of any $x \in A$ (the input to the hash function) and of $y \in B$ (the **checksum**).

      (2 marks)

ii. In a hash function h, what is the situation termed where $x, x' \in A$ such that $x \neq x'$ and $h(x) = h(x')$ and what does it mean?

(2 marks)

iii. One of the properties required of a **cryptographic hash function** is that it is computationally infeasible to find two inputs $x, x' \in A$ such that $x \neq x'$ and $h(x) = h(x')$

In recent years it has been discovered that this property does not hold for the cryptographic hash function **MD5**. MD5 has been widely used by CAs issuing digital certificates. How might an attacker **exploit** this weakness of MD5?

(3 marks)

4. a) Describe the three components of an **authentication system**

(3 marks)

b) Early versions of **Unix** used a password-based authentication system in which the users' password checksums were stored in the file ***/etc/passwd*** which was readable by any user.

i. Identify each of the three components from part (a) as they applied to early Unix.

(3 marks)

ii. What is the primary **vulnerability** of this **authentication system**, and why was it not considered significant when Unix first appeared?

(2 marks

iii. What kind of **attack** has proven to be the greatest **threat** to this **vulnerability** and, in broad terms, how would it be carried out?

(2 marks)

iv. When a user is prompted to choose a new password, many modern computer systems will evaluate the user's password choice for **strength**. One of the checks such a system might do is call a **spell checker**. Why is this?

(2 marks)

c) A thief steals a smartphone that **authenticates** its owner using a **4-digit PIN**, with no disabling, jailing or exponential back-off for making too many failed authentication attempts. Using **Anderson's formula**, what is the probability that an attacker is able to log into the phone within 3 hours? Assume that the thief is able to try one **PIN** every 2 seconds.

(5 marks)

d) A password or PIN is **something the user knows**. What are the other three **characteristics** that an authentication system may use, and give one example of each.

(3 marks)

e) **Multi-factor authentication** uses two or more of the above characteristics in combination. For purchasing goods, state which of the following means of authenticating the purchaser use multi-factor authentication. For each, state which factors or characteristics they use:

(3 marks)

i. Paper cheque

ii. Chip-and-PIN debit card

iii. Touch-and-go debit card

f) Of the methods of payment in (e), which offers the least security for the account holder? Give your reasons.

(2 marks)

5. a) In a **multi-tasking operating system**, why is **memory management** needed and why is it a security issue?

(5 marks)

b) Imagine you are responsible for writing a subroutine that **authenticates** a user's password. You read the password typed by the user into a variable called `psswd`. When the password has been verified and before the subroutine exits, what should your code do and why?

(3 marks)

c) Eve follows Bob on **Twitter** in order to collect personal information about him. This allows Eve to find out where Bob works and then guess the **login credentials** for Bob's user account on his work computer. Eve then logs in to Bob's work computer remotely as Bob and downloads **malware** that she has disguised to look like a **security patch** from a reputable software vendor. The **auto-update** software installs the software, the effect of which it to overwrite key operating system functions and install a **zombie**. Now Bob's computer is complicit in compromising the **availability** of a server on the other side of the world. Use your knowledge of Information Security to speculate plausibly about what vulnerabilities Eve is exploiting, and the kinds of attacks she is using.

(6 marks)

d) Consider a **SYN Flood** distributed denial-of-service (**DDoS**) attack in which 25 agent zombies are continually sending **30-byte SYN packets** to an on-line betting site comprising **100** servers. Each server maintains a connection table with a capacity of up to **512** TCP connections. A server will send a **SYN-ACK** packet four times, at **t = 32s** time intervals, then purge the request from the table.

i. At what **rate** will the **SYN packets** fill all the connection tables?

(2 marks)

ii. At what **rate** must each zombie issue **SYN packets**?

(2 marks)

iii. How much **bandwidth** is required for each **zombie** in order to achieve (ii)?

(2 marks)

e) A variant of the **SYN Flood** attack is a **SYN Spoofing** attack. What is the key characteristic of SYN Spoofing?

(3 marks).

f) Why might a **SYN Spoofing** attack be more successful than a conventional SYN Flood attack?

(2 marks)

END OF EXAMINATION PAPER