Unit 6 · Secrets and Security

WORKSHEET

Full marks 34

Name _____ Class _____ Roll no. ____ Date _____ Marks _____ / 34

1 Key words [4]

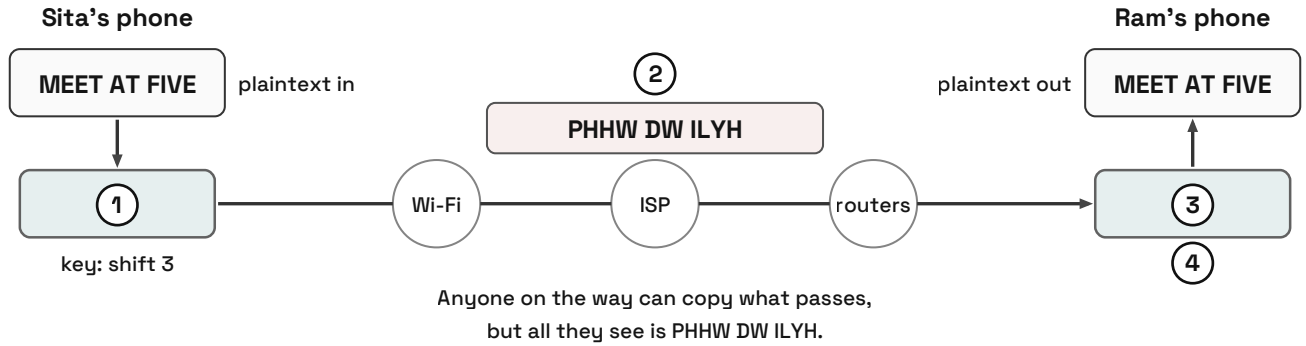
Fill in the blanks with words from the box. Two words in the box are not needed. Each blank carries 0.5 mark.

brute-force attack	ciphertext	digital signature	firewall	frequency analysis	hash	key	salt	social engineering	tailgating

The scrambled message that crosses the network is the _____. The secret that a cipher uses is its _____. Trying every possible key is a _____. Counting how often each letter comes in a ciphertext is _____. A _____ is a short, fixed-size value worked out from any data, and it can't be turned back. A few random characters added to each password before it is hashed are a _____. Something made with a private key that anyone can check with the public key is a _____. Tricking people into giving away secrets, instead of breaking the technology, is _____.

2 Label the diagram [2]

The diagram shows Sita's message crossing the network. Write the word that belongs in place of 1 to 4. Each carries 0.5 mark.



1. _____ 2. _____

3. _____ 4. _____

3 Multiple choice [5]

Choose the correct option for each of the following questions.

i. With a shift of 5, what does the letter W become? [1]

a. A b. B

c. C d. Z

ii. Why does frequency analysis work on a substitution cipher? **[1]**

a. Its key is always the shift 3.

b. Each plain letter always becomes the same secret letter, so the ciphertext keeps the pattern of how often each letter is used.

c. It has only 25 keys.

d. It doesn't change the spaces, so the words can be read.

iii. A cipher's key is made 10 bits longer. How many times longer does a brute-force attack take? **[1]**

a. 10 times **b.** 20 times

c. 100 times **d.** 1,024 times

iv. Hari and Gita both use the password **sunflower123** on a website that salts its hashes. What is true? **[1]**

a. They have the same stored hash.

b. Their stored hashes are different, because each has a different salt.

c. The website stores the salt as a secret, hidden from everyone.

d. The salt makes their password stronger against guessing at the login page.

v. You open **https://bhakaripay-reward.com** from a message. The page has a padlock and a valid certificate. What does that tell you? **[1]**

a. that it is Bhakari Pay's real website

b. that the page is honest and safe

c. only that your connection to whoever owns bhakaripay-reward.com is encrypted

d. that the government has checked the page

4 What does it print? [3]

Write exactly what the program prints, in the box under it.

A website stored this hash when Sita signed up with the password **tiger rice window** and the salt **k7Qp2x**.

```
import hashlib

def sha256(text):
    return hashlib.sha256(text.encode()).hexdigest()

stored = sha256("k7Qp2x" + "tiger rice window")
print(len(stored))
print(sha256("k7Qp2x" + "tiger rice window") == stored)
print(sha256("k7Qp2x" + "Tiger rice window") == stored)
print(sha256("p2xk7Q" + "tiger rice window") == stored)
```

OUTPUT

5 Trace the program [4]

Fill in the trace table: one row for each time round the loop, then what the program prints. The first row shows the values before the loop.

This program decrypts a Caesar cipher with a shift of 3.

```
ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
word = "BDN"
shift = 3
result = ""
for ch in word:
    i = ALPHABET.index(ch)
    j = (i - shift) % 26
    result = result + ALPHABET[j]
print(result)
```

ch	i	j	result	Output
(before)			""	

6 Find and fix the bug [3]

Read the program, then answer.

This program should encrypt with a Caesar cipher. It prints `QDPDVWH` for the first message, then stops with an error.

```
ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

def caesar(text, shift):
    result = ""
    for ch in text.upper():
        if ch in ALPHABET:
            i = ALPHABET.index(ch)
            result = result + ALPHABET[i + shift]
        else:
            result = result + ch
    return result

print(caesar("Namaste", 3))
print(caesar("Tiger zoo", 3))
```

i. Which line stops the program, and with which error?

ii. Why does the second message fail when the first one worked?

iii. Write the corrected line.

7 Write a program [4]

Write the program in Python on the lines. Any program that gives the right result gets the marks.

Write a program that asks for a ciphertext, counts how often each letter A to Z comes in it, and prints the commonest letter and how many times it comes. Then, guessing that it stands for E, print the shift. For `AOL LEHT YLZBSAZ DPSS IL WBA BW VU AOL UVAPJL IVHYK` it should print `Commonest: L 6 times` and `If it stands for E, the shift is 7`.

8 Short answers [3]

Write short answers to the following questions.

A school's login page builds its database command like this:

```
query = "SELECT * FROM users WHERE name = '" + name + "' AND password = '" +
password + "'"
```

i. What is the kind of attack this allows called, and what makes it possible?
ii. How should the program send the command and what the user typed?
iii. The command shows a second flaw. What is it, and what should the website do instead?

9 Long answer [4]

Write a long answer to the following question.

A family shop in Hetauda takes payments by QR code on the owner's phone. The phone has no screen lock, because "it is faster to sell". The wallet app's PIN is 1234. The owner's son installs games from links friends send him on the same phone, and there is no backup of the shop's accounts, kept in a notes app. Propose a fix for each flaw, and say what each fix costs the family.

10 Think [2]

Think, then answer.

Police in many countries ask messaging companies to let them read the messages of criminals. Why do security experts say that a "door for the police" in end-to-end encryption is dangerous?

11 Activity: Break your partner's cipher (not marked)

Work in pairs, on paper. Each of you writes two sentences of English (at least 60 letters), encrypts them with a Caesar cipher and a secret shift, and gives the ciphertext to your partner. Break your partner's ciphertext by counting the letters, without being told the shift. Then check your answer with the activity **Crack it without the key** on the unit's page (the QR code).

	My partner's ciphertext	Commonest letter, how many times	Shift if it is E	English? If not, the shift I found
Try 1				
Try 2				