Unit 6 · Secrets and Security

ANSWER KEY · FOR TEACHERS

Full marks 34

Give the marks for the points in the marking scheme; an answer in other words that says the same is right.

1 Key words

1. ciphertext
2. key
3. brute-force attack
4. frequency analysis
5. hash
6. salt
7. digital signature
8. social engineering

Each carries 0.5 mark. **K · 4**

2 Label the diagram

1. encrypt
2. ciphertext
3. decrypt
4. the same key

Each carries 0.5 mark. **U · 2**

3 Multiple choice

i. **b. B** **A · 1**

W is at position 22 (counting A as 0). 22 + 5 = 27, and 27 % 26 = 1, which is B. Counting on the fingers: X, Y, Z, A, B.

ii. **b. Each plain letter always becomes the same secret letter, so the ciphertext keeps the pattern of how often each letter is used.** **U · 1**

Swapping letters changes what they look like, but not how often they appear. If E is about one letter in eight of English, its secret letter is about one letter in eight of the ciphertext. (The kept spaces help too, as they show the shapes of words, but the counting works even without them.)

iii. **d. 1,024 times** **U · 1**

Each bit doubles the number of keys, so 10 bits multiply it by $2^{10} = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 1{,}024$. That is why key lengths jump from 56 to 128 to 256 bits: each step is enormous.

iv. **b. Their stored hashes are different, because each has a different salt.** **A · 1**

Each user gets a random salt, so the same password gives different hashes. The salt isn't secret: it is stored beside the hash. It doesn't make a weak password harder to guess one at a time; it stops one guess cracking many users at once, and stops ready-made lists. (sunflower123 is still a weak password.)

v. **c. only that your connection to whoever owns bhakaripay-reward.com is encrypted** **A · 1**

The certificate proves the connection is to the owner of the name bhakaripay-reward.com, and nobody on the way can read it. Anyone can buy that name and get a certificate for it. Read the owner's name (Grade 7): it is bhakaripay-reward, not bhakaripay.com.np. And open the app yourself instead of tapping links.

Science Playground, Katunje, Bhaktapur
Book a class visit: https://science-playground.com/booking

4 What does it print?

MARKING SCHEME U · 3

- ✓ `64`: a SHA-256 hash is always 64 hex digits.
- ✓ `True`: the same salt and password always give the same hash.
- ✓ `False` and `False`: one capital letter, or a different salt, gives a completely different hash.

5 Trace the program

ANSWER A · 4

`ch`	`i`	`j`	`result`	**Output**
(before)			""	
`B`	1	24	"Y"	
`D`	3	0	"YA"	
`N`	13	10	"YAK"	
				YAK

MARKING SCHEME

- ✓ `i` 1, 3, 13: each letter's position, counting A as 0.
- ✓ `j` 24 for B: 1 − 3 = −2, and `-2 % 26` is 24, so the alphabet wraps round to Y.
- ✓ `j` 0 and 10, and `result` growing "Y", "YA", "YAK".
- ✓ Output `YAK`, once, after the loop.

6 Find and fix the bug

MARKING SCHEME A · 3

- ✓ Line 8, an IndexError.
- ✓ The Z in "zoo": 25 + 3 = 28 is past the last position, 25; the alphabet doesn't wrap round.
- ✓ `ALPHABET[(i + shift) % 26]` (`% 26` gives the wrap-around).

Science Playground, Katunje, Bhaktapur
Book a class visit: https://science-playground.com/booking

7 Write a program

ANSWER A · 4

```
ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
secret = input("Ciphertext: ")
counts = {}
for ch in secret.upper():
    if ch in ALPHABET:
        counts[ch] = counts.get(ch, 0) + 1
top = ""
for letter in counts:
    if top == "" or counts[letter] > counts[top]:
        top = letter
print("Commonest:", top, counts[top], "times")
shift = (ALPHABET.index(top) - ALPHABET.index("E")) % 26
print("If it stands for E, the shift is", shift)
```

OUTPUT

```
Ciphertext: AOL LEHT YLZBSAZ DPSS IL WBA BW VU AOL UVAPJL IVHYK
Commonest: L 6 times
If it stands for E, the shift is 7
```

Other right ways: a list of 26 counts indexed by each letter's position, or `max(counts, key=counts.get)` for the commonest.

MARKING SCHEME

- ✓ The ciphertext read with `input()`, and only the letters counted (spaces left out).
- ✓ A count for each letter, kept in a dictionary (or a list of 26).
- ✓ The commonest letter found and printed with its count.
- ✓ The shift worked out as the commonest letter's position minus E's (L is 11, E is 4: 7), wrapped with `% 26`.

8 Short answers

MARKING SCHEME A · 3

- ✓ SQL injection, because the input is joined into the command and treated as part of it.
- ✓ The command with placeholders, and the input sent separately (so it is only ever data).
- ✓ Passwords are stored as they are; store a salted, slow hash and compare hashes instead.

9 Long answer

ANSWER

Flaw	Fix	Its price
no screen lock	a screen lock with a fingerprint or face, quick to open	a second each time; the owner must not share the PIN
wallet PIN 1234	a PIN nobody can guess (not a birthday or a pattern), and the wallet's own fingerprint lock	remembering a new PIN
games installed from links	install apps only from the app store; better, the son uses another phone, or a separate user on it	the son's convenience; perhaps the cost of a cheap second phone
no backup of the accounts	a backup of the notes to an online account, automatic, and a copy written in a register once a week	a little time; online space

Science Playground, Katunje, Bhaktapur
Book a class visit: https://science-playground.com/booking

The most urgent: stop installing apps from links (it could put malware next to the wallet) and add the screen lock; both cost almost nothing. A shop's payments phone protects the family's income, so it deserves the strongest protection the family owns. A · 4

MARKING SCHEME

- ✓ No screen lock: add a screen lock with a fingerprint or face; it costs a second each time.
- ✓ Wallet PIN 1234: a PIN nobody can guess, or the wallet's fingerprint lock; it costs remembering a new PIN.
- ✓ Games from links: apps only from the app store, or the son uses another phone or user; it costs the son's convenience, perhaps a cheap phone.
- ✓ No backup: an automatic online backup and a copy in a register; it costs a little time and space.

10 Think

ANSWER HA · 2

A way in for the police is a way in that exists, and anyone who finds or steals it can use it too: criminals, spies of other governments, or a dishonest employee. Mathematics can't tell a police officer from a thief, and a key that opens everyone's messages would be the most valuable secret in the world, very hard to keep safe forever. So there is no way to weaken encryption only for the good side. The other side is real too: criminals do use encrypted apps, so countries are still arguing about it.

MARKING SCHEME

- ✓ A door for the police is a door anyone who finds or steals it can use (criminals, other governments, a dishonest employee): encryption can't tell who is using it.
- ✓ Weighs the other side: it would help investigations, but it weakens everyone's privacy and safety.

11 Activity: Break your partner's cipher

(not marked)

WHAT STUDENTS SHOULD FIND

In most English sentences of 60 letters or more, the commonest letter of the ciphertext stands for E, so its distance from E is the shift. Sometimes it stands for T, A or O instead, and the shift gives nonsense: then try the next commonest letter, or try shifts one after another (brute force). The shorter the message, the more often the commonest letter misleads, which is why code breakers want as much ciphertext as they can get.

Marks by level	Knowledge	Understanding	Application	Higher ability	Total
Marks	4	7	21	2	34

Science Playground, Katunje, Bhaktapur
Book a class visit: https://science-playground.com/booking