Unit 7 · Cryptography and Trust

ANSWER KEY · FOR TEACHERS

Full marks 31

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. modulus
2. inverse
3. padding
4. discrete logarithm
5. forward secrecy
6. replay
7. nonce
8. Kerckhoffs's principle

Each carries 0.5 mark. **K · 4**

2 Multiple choice

i. **c.** Recompute block 3's hash and every block after it, and hope nobody kept a copy of the old last hash. **U · 1**

Block 4 holds block 3's old hash, so its link breaks; fixing it changes block 4's hash and breaks block 5, and so on to the end. Even then, anyone who kept the earlier last hash (published, or held by many copies) sees it differs.

ii. **b.** 7 **A · 1**

$3 \times 7 = 21$, and $21 \bmod 10 = 1$, so multiplying by 7 undoes multiplying by 3 on a clock of 10. ($3 \times 3 = 9$ and $3 \times 9 = 27$, which leave 9 and 7.) 3 does have an inverse, because 3 and 10 share no factor.

iii. **b.** She encrypts 1 and 2 herself with the public key and sees which matches. **U · 1**

Encrypting needs only the public key, and textbook RSA always gives the same ciphertext for the same message. With only two possible messages, Eve doesn't need to decrypt at all. Random padding stops this: each encryption of 1 looks different.

iv. **b.** Only that the owner of the key signed this message at some time; the second copy could be a replay. **U · 1**

A copy of a signed message has the same signature, and still checks. Only a date or a number used once, inside what was signed, lets the receiver refuse the second copy. Nothing about the copy suggests the key was stolen: anyone can copy a message.

v. **b.** A bank uses a published, well-studied method and keeps only its keys secret. **U · 1**

The method will be found out anyway; only the key can be kept secret, and replaced if it leaks. Published methods have been attacked by experts for years and survived, which a home-made one hasn't. A key inside an app is in every copy of the app.

3 Trace the program

ANSWER

`k` at the start	`result`	`square`	`k` at the end
13	3	2	6
6	3	4	3
3	5	2	1
1	3	4	0

It prints 3: $3^{13} \bmod 7$, since $13 = 8 + 4 + 1$ and $3 \times 4 \times 2 = 24$ leaves 3.

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

MARKING SCHEME A · 4

- ✓ k 13, 6, 3, 1, then 0: halved each round, the remainder dropped.
- ✓ `result` changes only when k is odd: 1 × 3 = 3, then 3 × 4 = 12 → 5, then 5 × 2 = 10 → 3.
- ✓ `square` 2, 4, 2, 4: $3^2 = 9 \to 2$, $2^2 = 4$, $4^2 = 16 \to 2$, $2^2 = 4$.
- ✓ Output 3.

4 What does it print?

MARKING SCHEME A · 3

- ✓ `sent: 8 7`: $2^3 = 8$, and $2^7 = 128 = 11 \times 11 + 7$.
- ✓ `keys: 2 2`: $7^3 = 343 = 31 \times 11 + 2$, and $8^7 = 2^{21}$ leaves 2 as well: both get the same key.
- ✓ `Eve multiplies: 1`: $56 = 5 \times 11 + 1$. Combining the numbers she saw doesn't give the key.

5 A small key protects nothing

ANSWER A · 4

i. Trying small primes: 221 ÷ 13 = 17, so **221 = 13 × 17**, and **φ(n) = 12 × 16 = 192.**

ii. d is the inverse of 5, mod 192: 5d must be 1 more than a multiple of 192. 192 + 1 = 193 doesn't divide by 5; 2 × 192 + 1 = 385 = 5 × 77. So **d = 77.** Check: 5 × 77 = 385 = 2 × 192 + 1.

iii. $c = 10^5 \bmod 221 = 100{,}000 \bmod 221$. 221 × 452 = 99,892, so **c = 108.** (Decrypting, $108^{77} \bmod 221$ gives 10 again.)

iv. A real n is at least 2,048 bits, 617 digits: trying divisors one by one would take about 10^{308} tries, and even the best methods known can't factor a number that size. Without p and q there is no φ(n), and without φ(n) no d.

MARKING SCHEME

- ✓ 221 = 13 × 17, and φ(n) = 12 × 16 = 192.
- ✓ d = 77, checked: 5 × 77 = 385 = 2 × 192 + 1.
- ✓ c = 100,000 mod 221 = 108.
- ✓ A real n is hundreds of digits long, and no known method factors it in any reasonable time.

6 Review the code

MARKING SCHEME A · 3

- ✓ Line 5, the private key in the code: it leaks with every copy, backup and history; keep it in the server's settings or a secrets store.
- ✓ Line 11, `random` for a session ID: predictable; use `secrets.token_urlsafe()`.
- ✓ Lines 14–15, a check that can be skipped by an old date: refuse unsigned notices (and sign the old ones again).

7 Short answer

MARKING SCHEME U · 2

- ✓ It proves who: it was signed with the private key matching that public key; and that the message is unchanged, to the last character.
- ✓ Any two it doesn't: which person holds the key; that the key wasn't stolen; that the message is true; when it was signed, or that it isn't a replay.

8 Long answer

ANSWER

It would help with: records can't be changed quietly after they are entered (each change would break the chain, and many copies hold the old hashes); and there is a clear, checkable history of every transfer.

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

It wouldn't help with: a false or mistaken record entered in the first place (by a corrupt or careless official, or with forged papers) stays forever; it can't check who really occupies the land; it makes honest corrections harder; and if the keys used to approve transfers are stolen, the thief's transfers are just as permanent.
Advice: the municipality is already the trusted keeper, so a well-run database with signed entries, backups in several places, audit logs, and the latest hash published regularly (on its website and in a newspaper) gives the same protection against quiet changes, far more cheaply. The real fraud risks are at the counter, where documents are checked, and need better procedures there. (Answers that recommend a blockchain must say who keeps the copies and why the parties can't trust one keeper.)

U · 4

MARKING SCHEME

- ✓ Two things it would solve: records can't be changed quietly after they are entered; a clear, checkable history of every transfer.
- ✓ Three it wouldn't: a false or mistaken record entered in the first place stays for ever; honest corrections become harder; a stolen approval key makes its transfers just as permanent (or: it can't check who really occupies the land).
- ✓ The municipality is already the trusted keeper, so a blockchain's many copies and cost buy little.
- ✓ Advice backed by a cheaper way: a database with signed entries, backups, audit logs and its last hash published regularly; the real fraud risk is at the counter, where papers are checked.

9 Think

ANSWER

HA · 2

The key never crosses the line: Sita and Ram each work it out at their own end, from the number they received and their own secret. What Eve hears (p, g, A and B) isn't enough without solving the discrete logarithm problem, which no known method does for primes hundreds of digits long. What she can do is stand in the middle and run a key exchange with each of them. That is stopped by a signature: the server signs its key-exchange number with the private key that matches its certificate, and Eve doesn't have it.

MARKING SCHEME

- ✓ The key is never sent: each side works it out from what it received and its own secret, and going back from A or B to a secret is the discrete logarithm problem.
- ✓ She could stand in the middle and exchange keys with each side; a signature on the key-exchange number, with the certificate's private key, stops her.

10 Activity: Agree on a key in public

(not marked)

WHAT STUDENTS SHOULD FIND

Sita and Ram always get the same key, whatever secrets they choose, though neither said theirs. Eve can find a secret only by working out 5^1, 5^2, 5^3 … mod 23 until one matches what she heard: with $p = 23$ she needs at most 22 tries, so she always succeeds, which shows why real primes are hundreds of digits long. For example, with secrets 6 and 4, Sita says 8, Ram says 4, and both get the key 2. Groups who check each other's arithmetic notice that one slip makes the two keys differ: real software checks this by using the key and seeing whether the other side can read the result.

Marks by level	Knowledge	Understanding	Application	Higher ability	Total
Marks	4	10	15	2	31

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