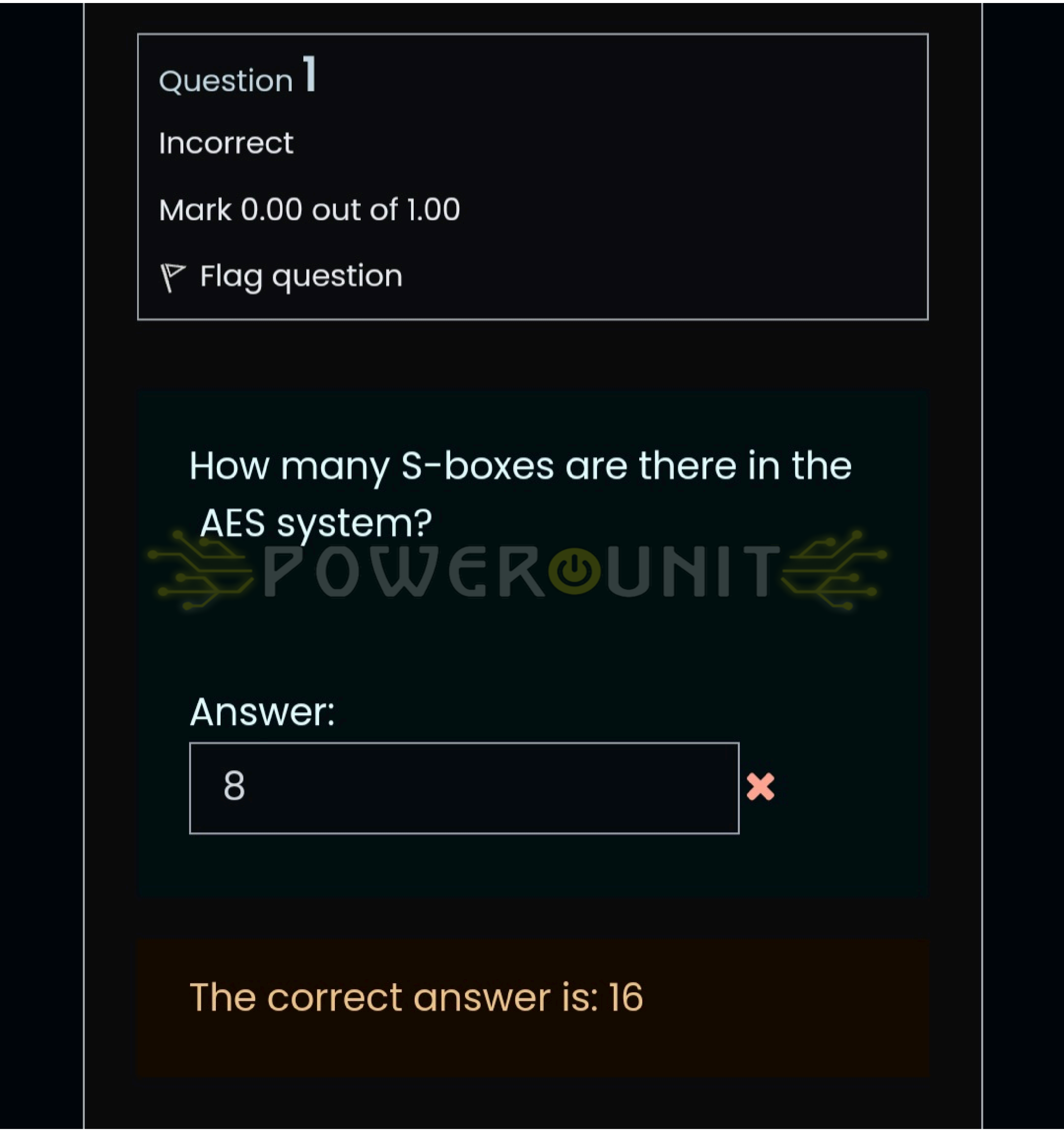


Question 1

Incorrect

Mark 0.00 out of 1.00

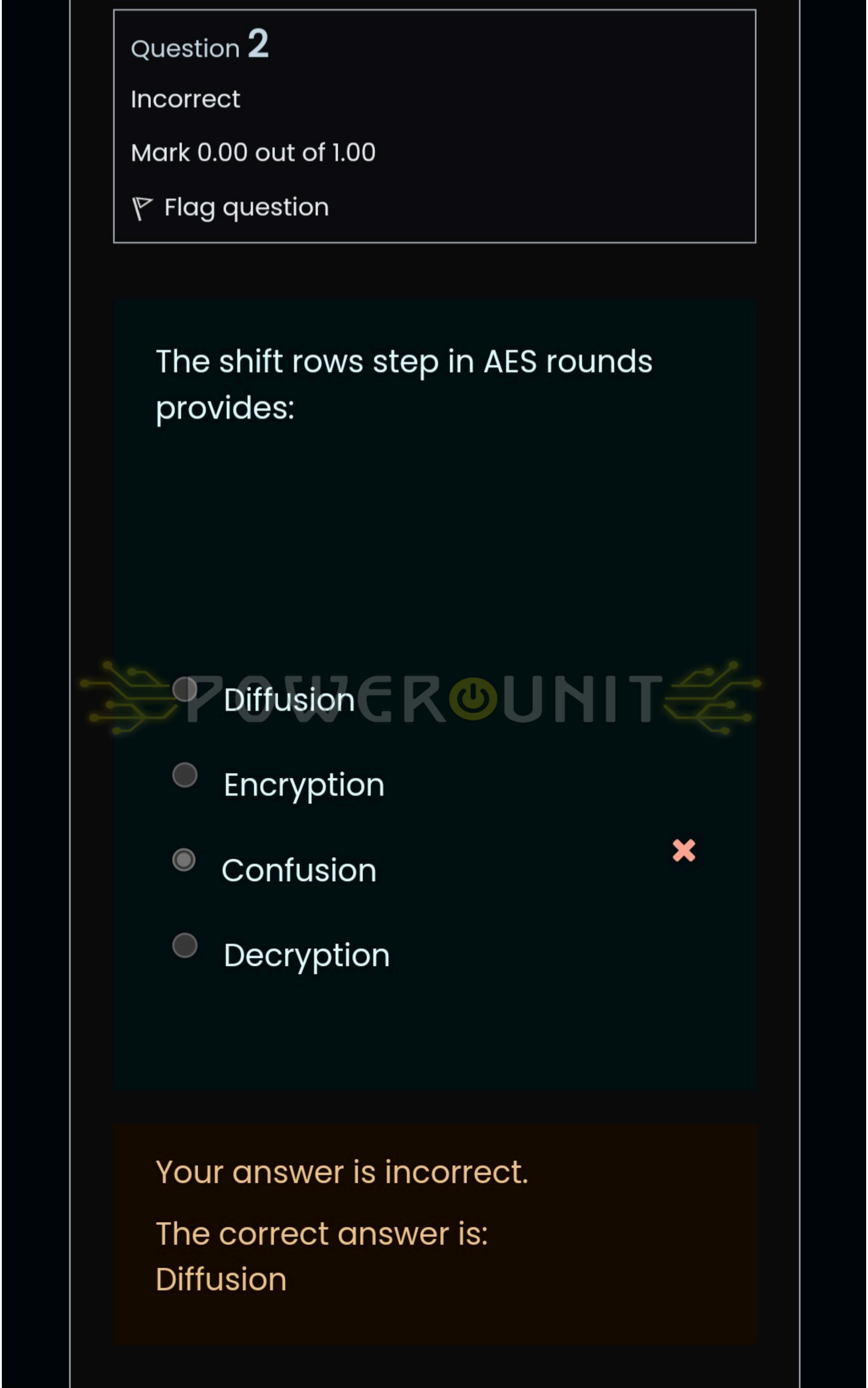
Flag question

How many S-boxes are there in the AES system?

Answer:

8 ✖

The correct answer is: 16



Question 2

Incorrect

Mark 0.00 out of 1.00

Flag question

The shift rows step in AES rounds provides:

○ Diffusion

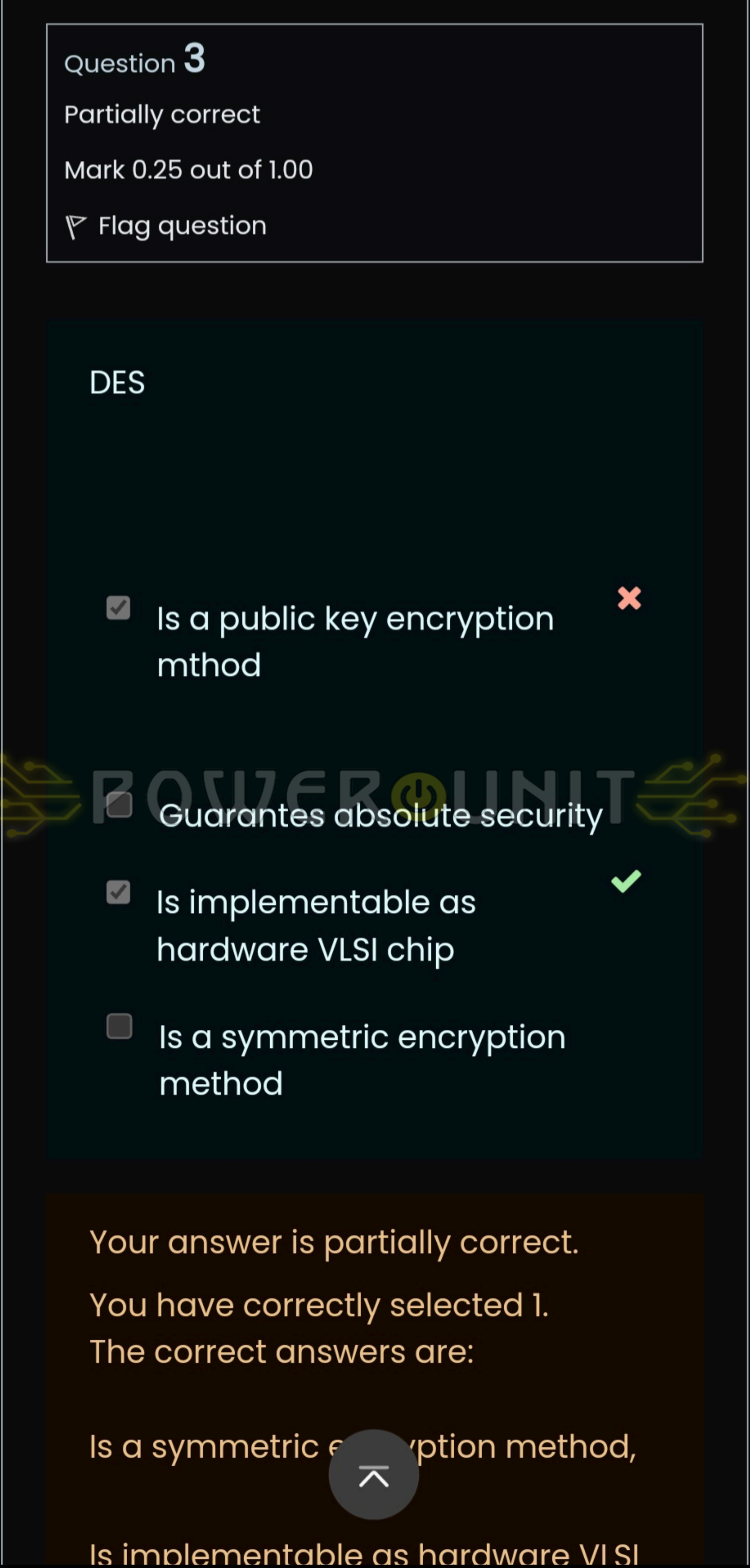
○ Encryption

● Confusion ✗

○ Decryption

Your answer is incorrect.

The correct answer is:
Diffusion



Question 3

Partially correct

Mark 0.25 out of 1.00

DES

☑ Is a public key encryption mthod ✗

□ Guarantes absolute security

☑ Is implementable as hardware VLSI chip ✓

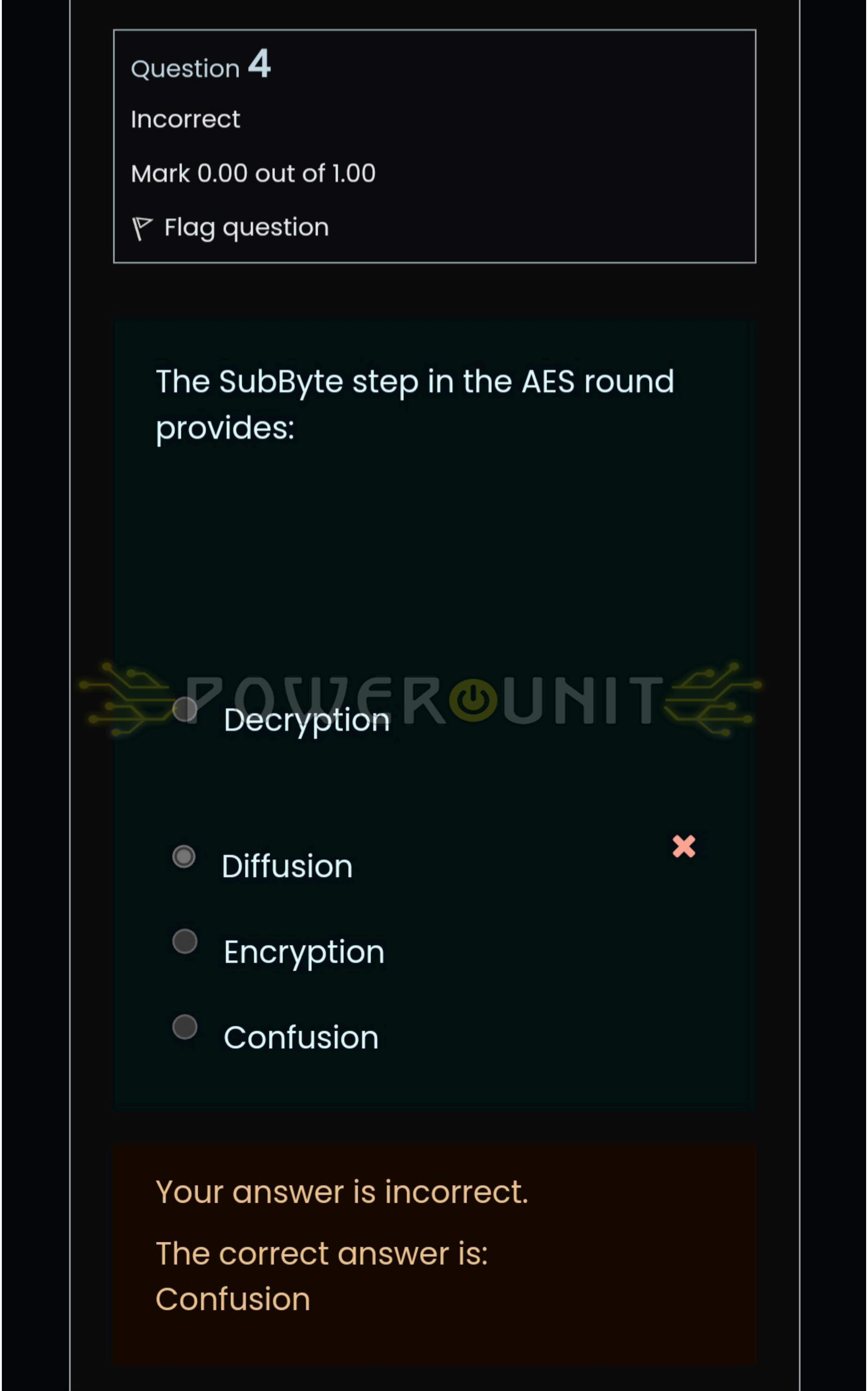
□ Is a symmetric encryption method

Your answer is partially correct.

You have correctly selected 1.
The correct answers are:

Is a symmetric encryption method,

Is implementable as hardware VLSI



Question 4

Incorrect

Mark 0.00 out of 1.00

Flag question

The SubByte step in the AES round provides:

○ Decryption

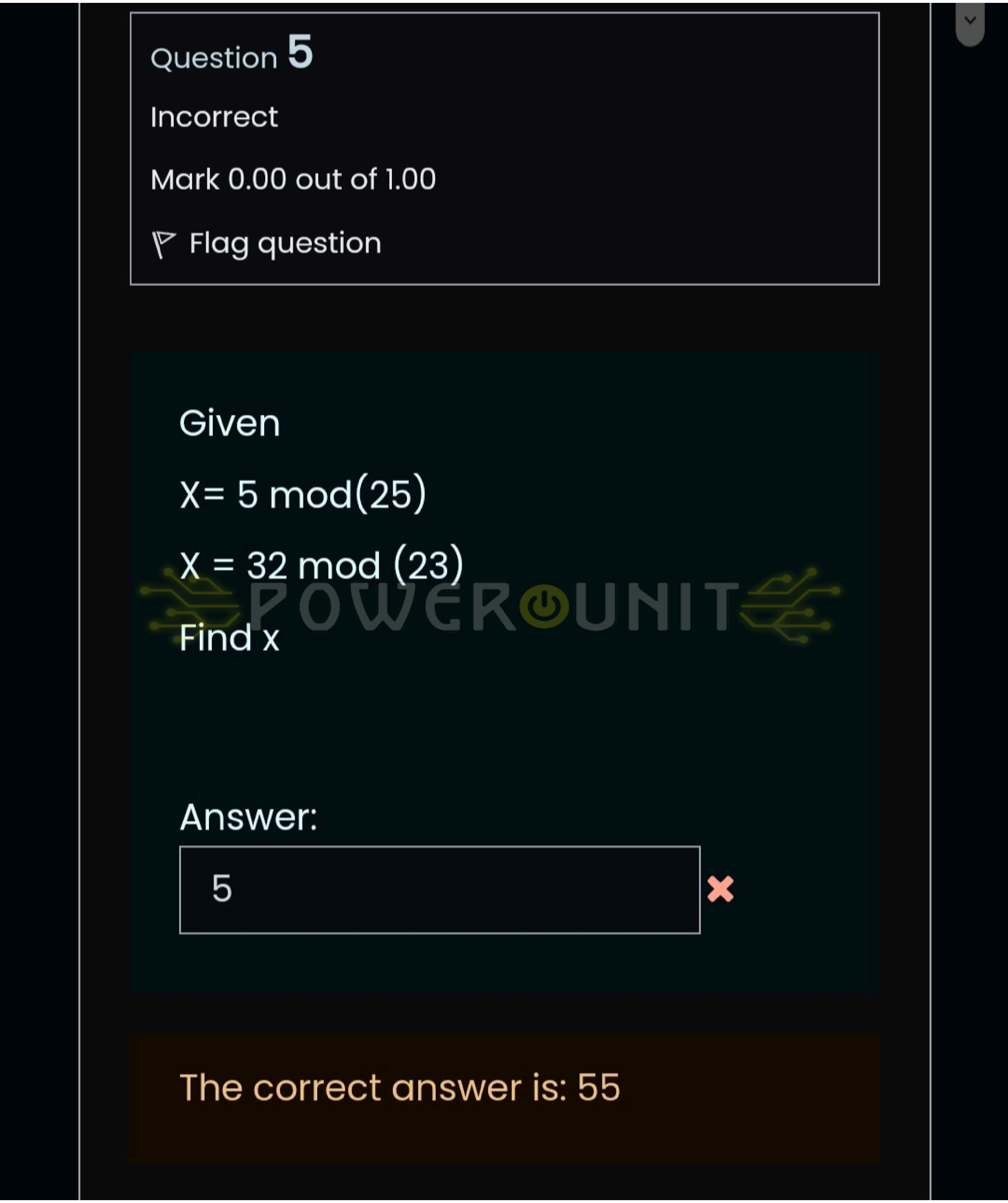
● Diffusion ✗

○ Encryption

○ Confusion

Your answer is incorrect.

The correct answer is:
Confusion



Question **5**

Incorrect

Mark 0.00 out of 1.00

Flag question

Given

X= 5 mod(25)

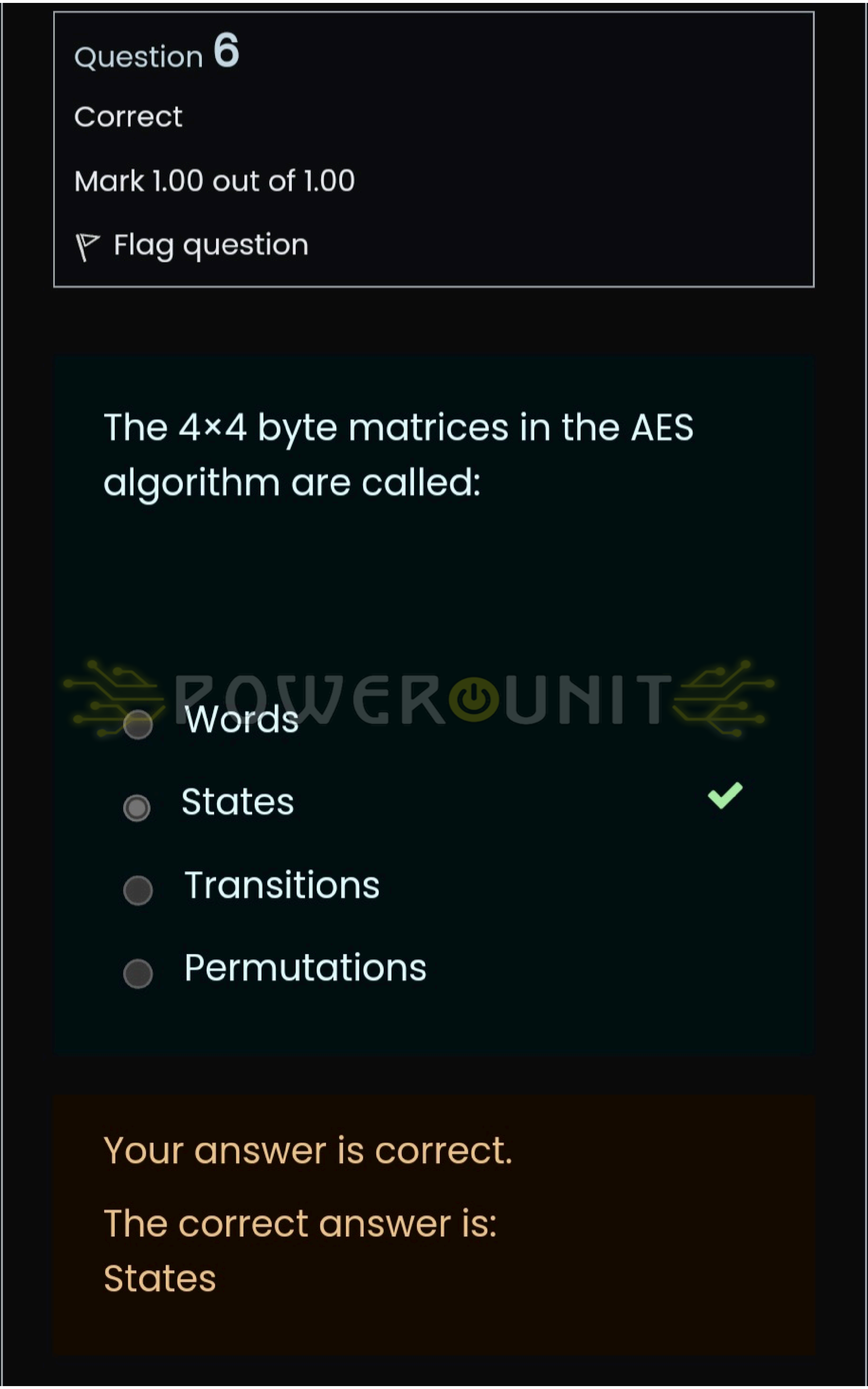
X = 32 mod (23)

Find x

Answer:

5 ✗

The correct answer is: 55



Question 6

Correct

Mark 1.00 out of 1.00

Flag question

The 4×4 byte matrices in the AES algorithm are called:

○ Words

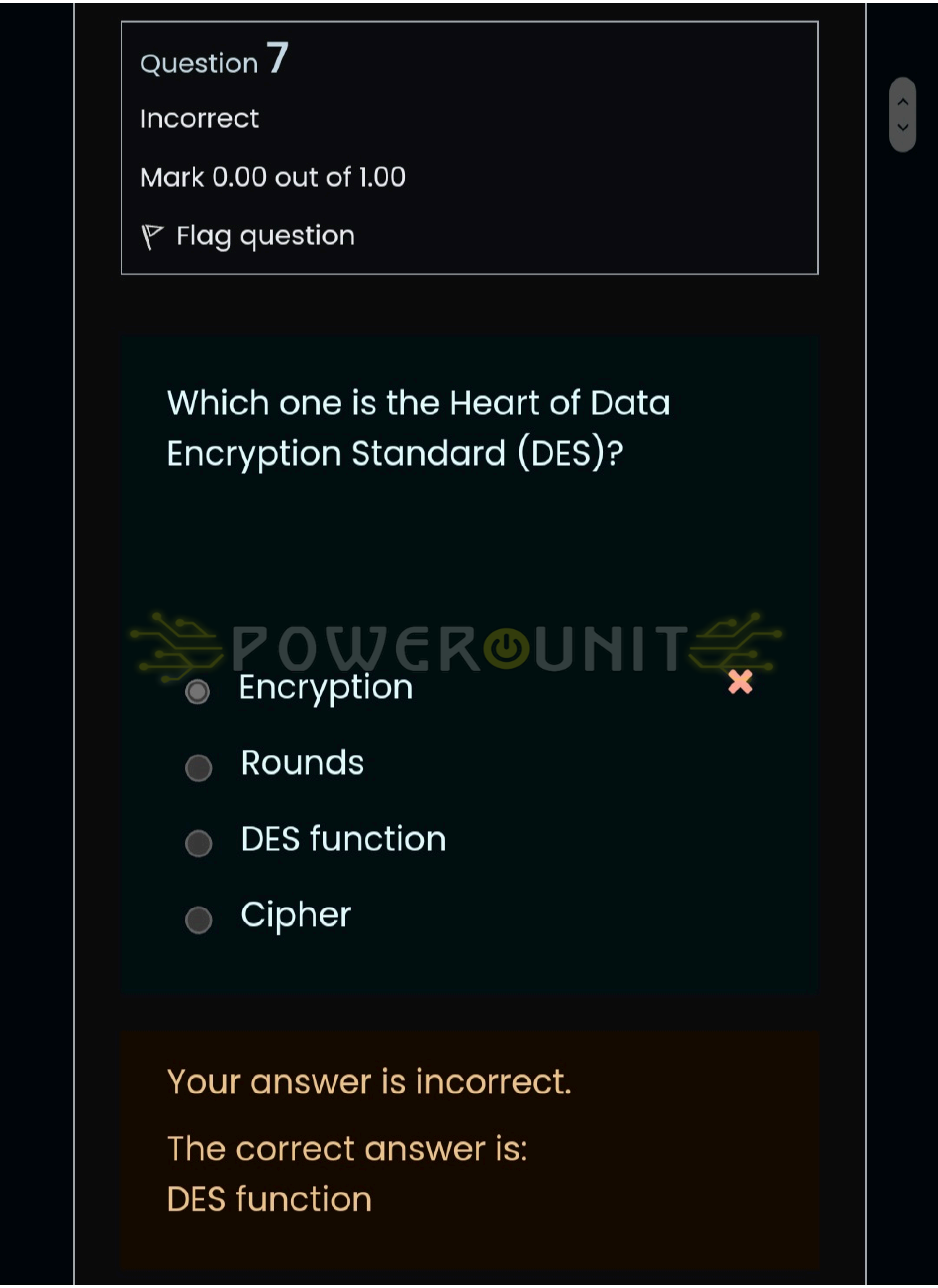
● States ✓

○ Transitions

○ Permutations

Your answer is correct.

The correct answer is:
States



Question 7

Incorrect

Mark 0.00 out of 1.00

Flag question

Which one is the Heart of Data Encryption Standard (DES)?

● Encryption ✗

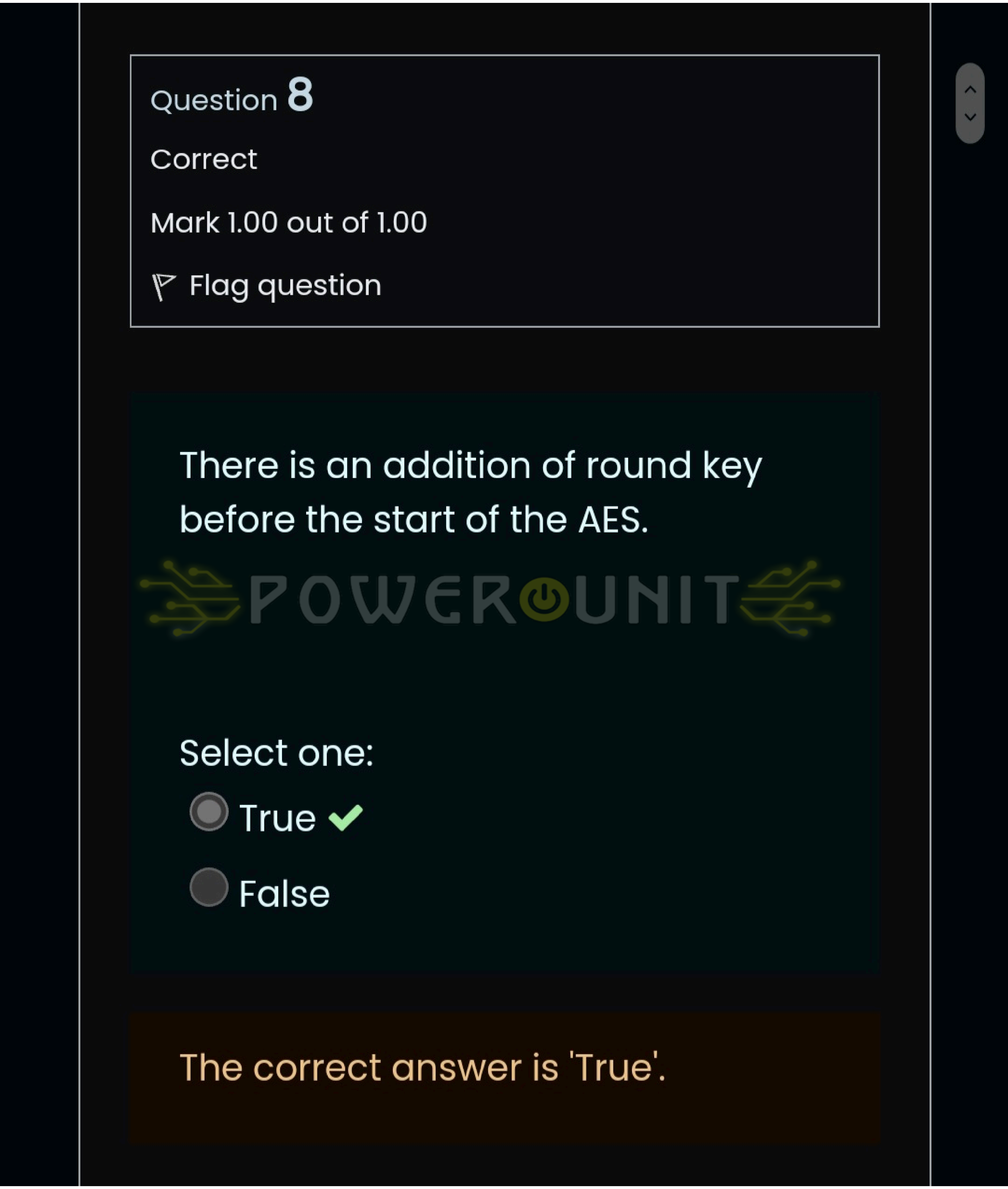
○ Rounds

○ DES function

○ Cipher

Your answer is incorrect.

The correct answer is:
DES function



Question 8

Correct

Mark 1.00 out of 1.00

Flag question

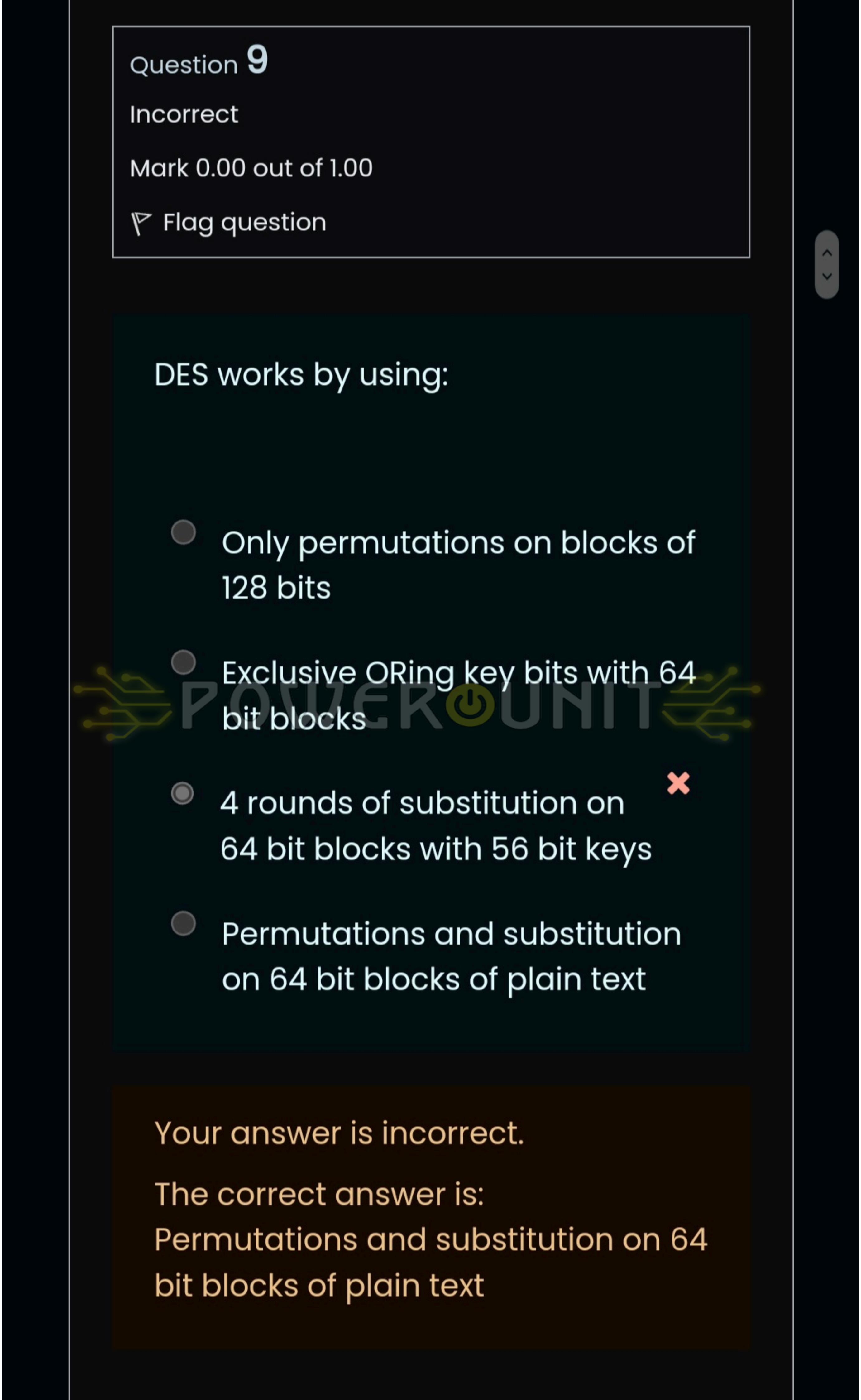
There is an addition of round key before the start of the AES.

Select one:

● True ✓

○ False

The correct answer is 'True'.



Question 9

Incorrect

Mark 0.00 out of 1.00

Flag question

DES works by using:

○ Only permutations on blocks of 128 bits

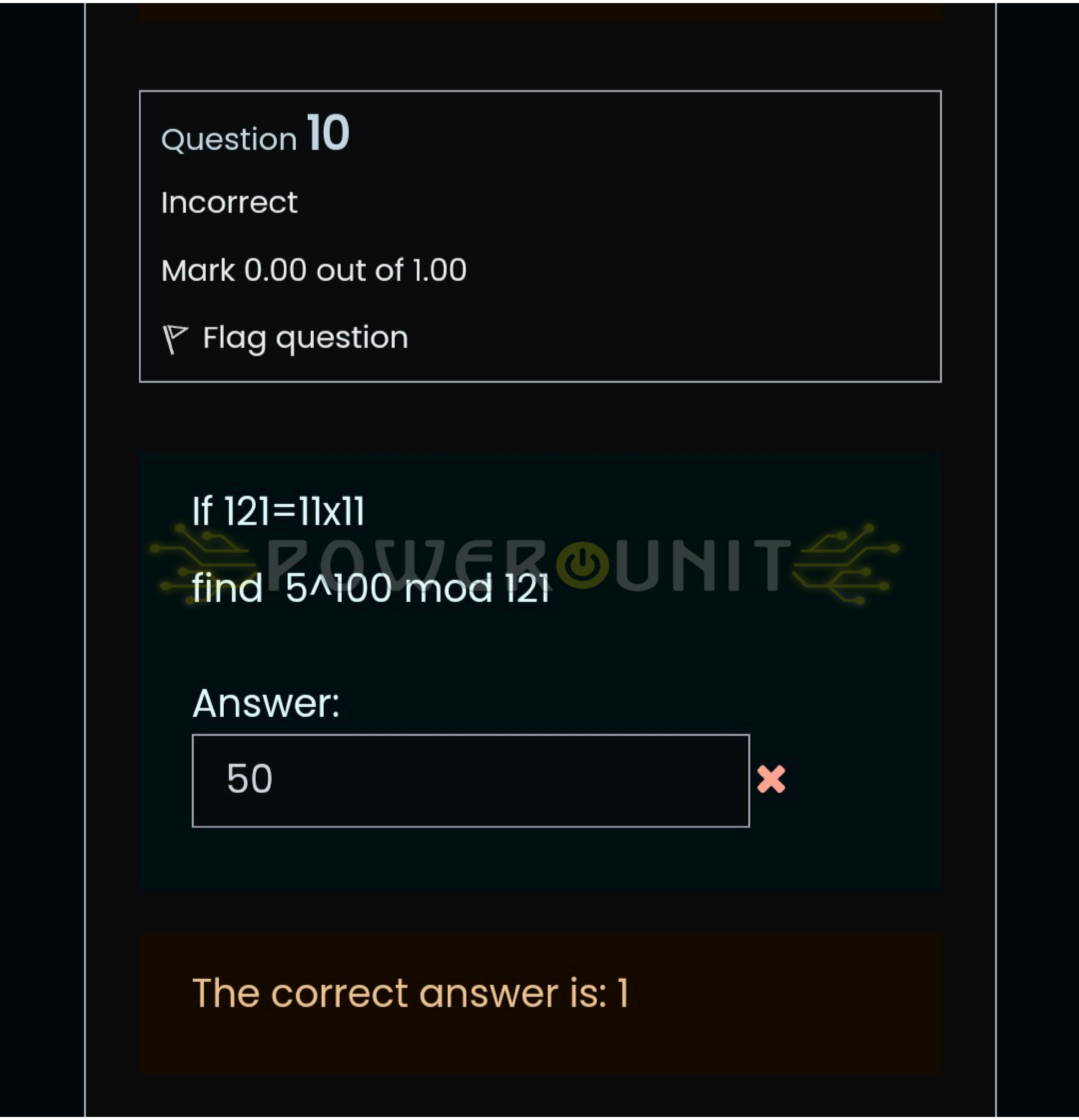
○ Exclusive ORing key bits with 64 bit blocks

● 4 rounds of substitution on 64 bit blocks with 56 bit keys ✖

○ Permutations and substitution on 64 bit blocks of plain text

Your answer is incorrect.

The correct answer is:
Permutations and substitution on 64 bit blocks of plain text



Question 10

Incorrect

Mark 0.00 out of 1.00

Flag question

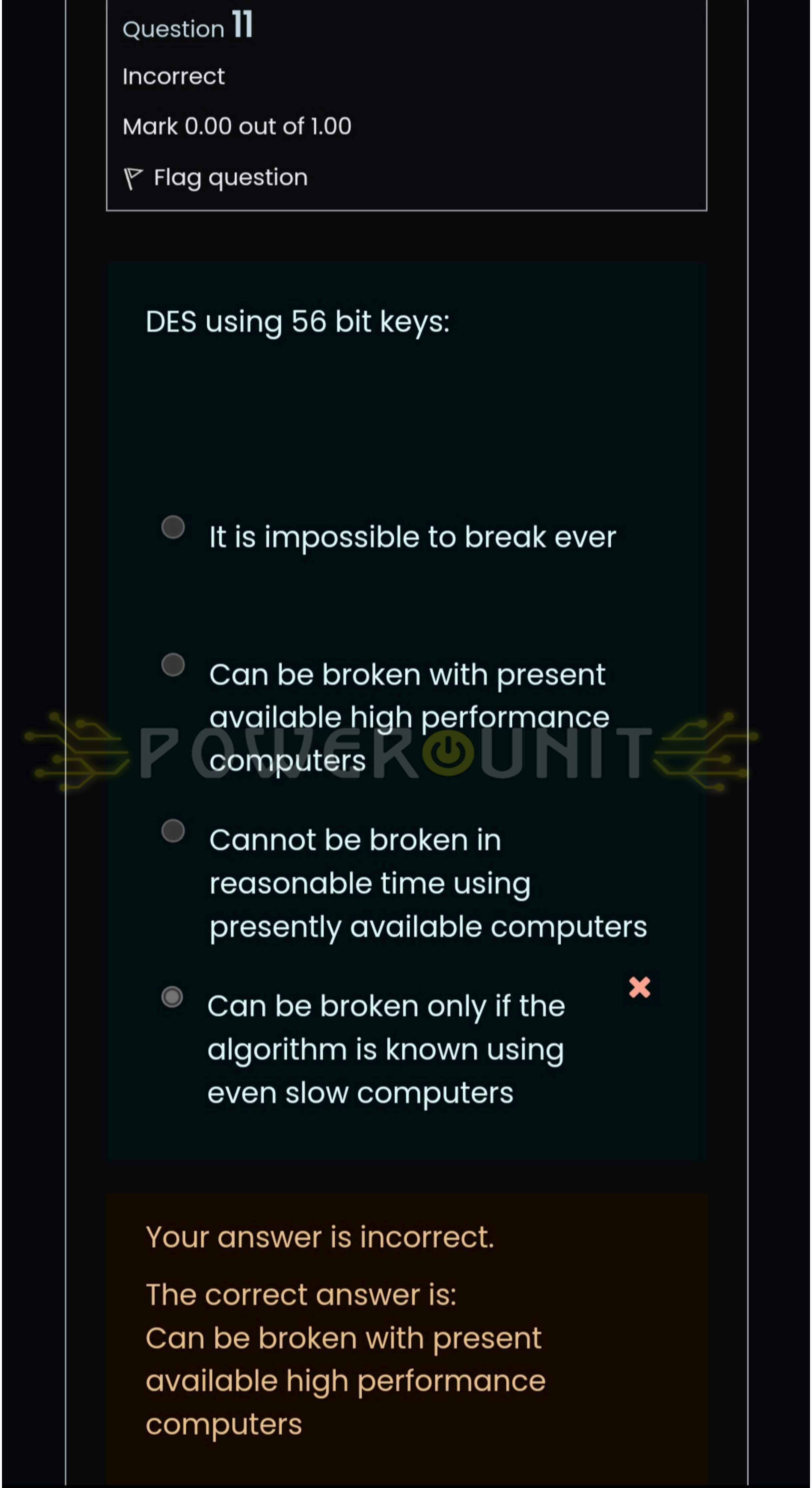
If 121=11x11

find 5^100 mod 121

Answer:

50 ✖

The correct answer is: 1



Question 11

Incorrect

Mark 0.00 out of 1.00

Flag question

DES using 56 bit keys:

○ It is impossible to break ever

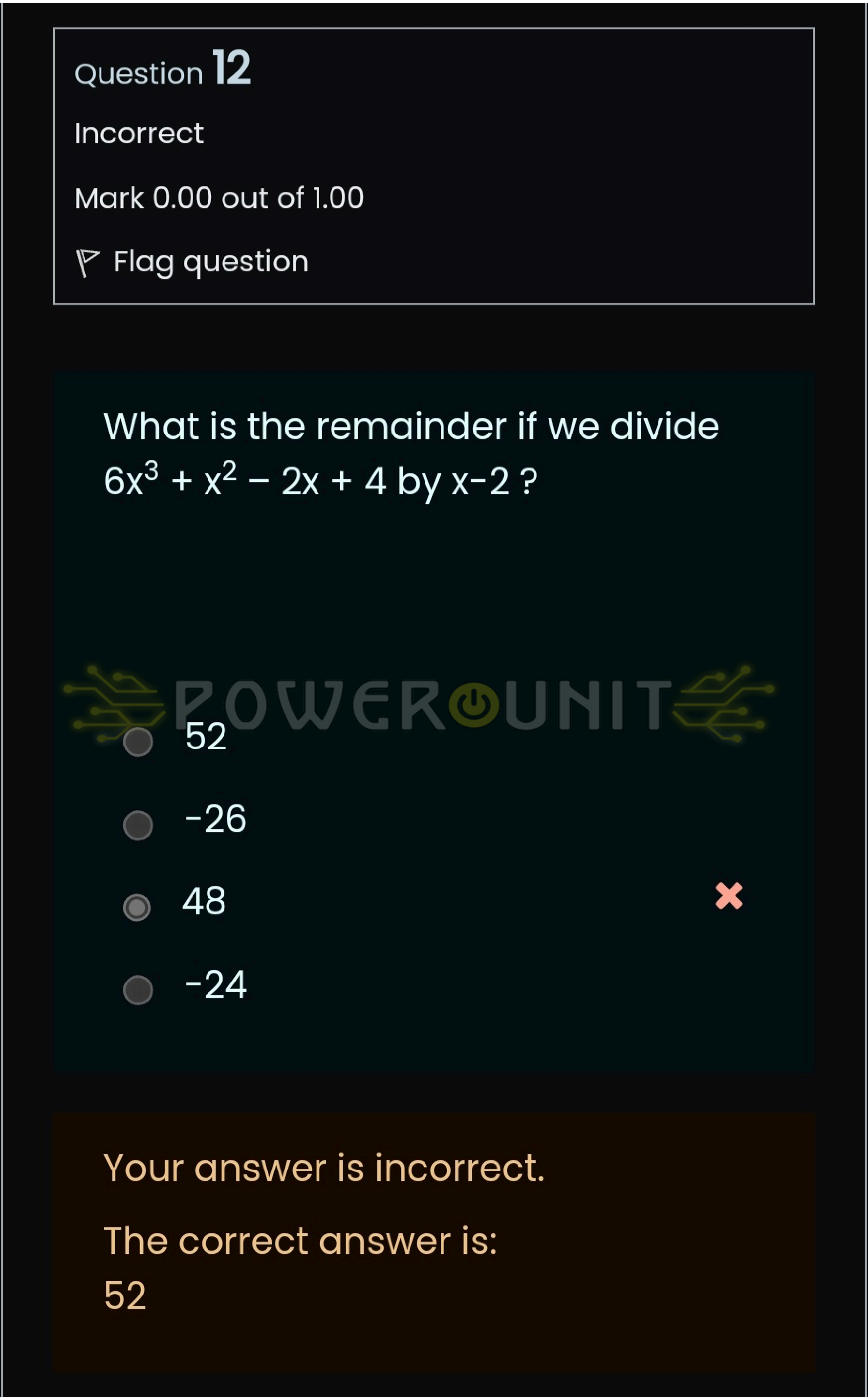
○ Can be broken with present available high performance computers

○ Cannot be broken in reasonable time using presently available computers

● Can be broken only if the algorithm is known using even slow computers ✖

Your answer is incorrect.

The correct answer is:
Can be broken with present available high performance computers



Question **12**

Incorrect

Mark 0.00 out of 1.00

Flag question

What is the remainder if we divide $6x^3 + x^2 - 2x + 4$ by x−2 ?

○ 52

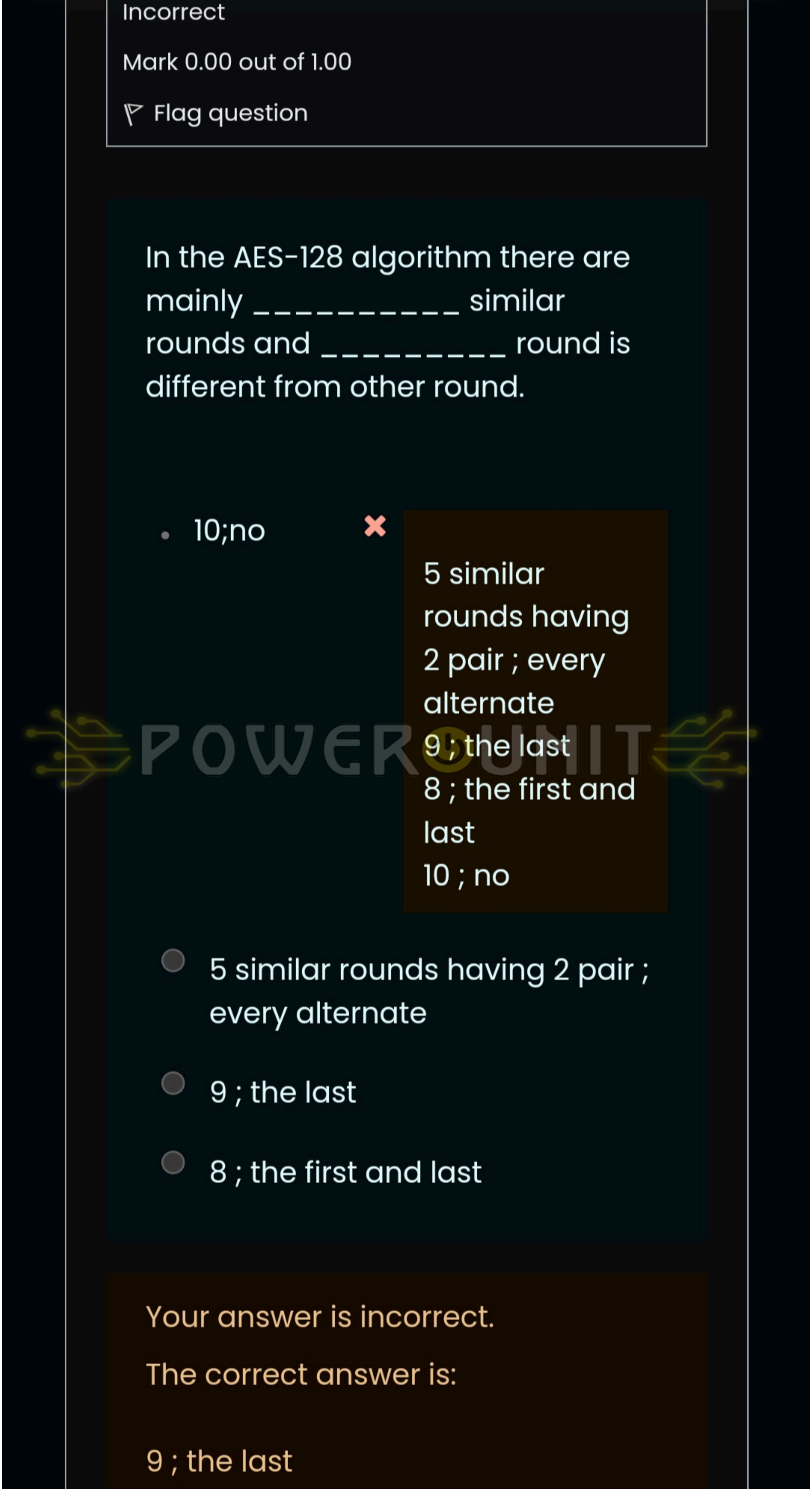
○ -26

● 48 ✗

○ -24

Your answer is incorrect.

The correct answer is:
52



Incorrect

Mark 0.00 out of 1.00

Flag question

In the AES-128 algorithm there are mainly ___________ similar rounds and __________ round is different from other round.

- 10;no ✗

5 similar rounds having 2 pair ; every alternate
9 ; the last
8 ; the first and last
10 ; no

○ 5 similar rounds having 2 pair ; every alternate

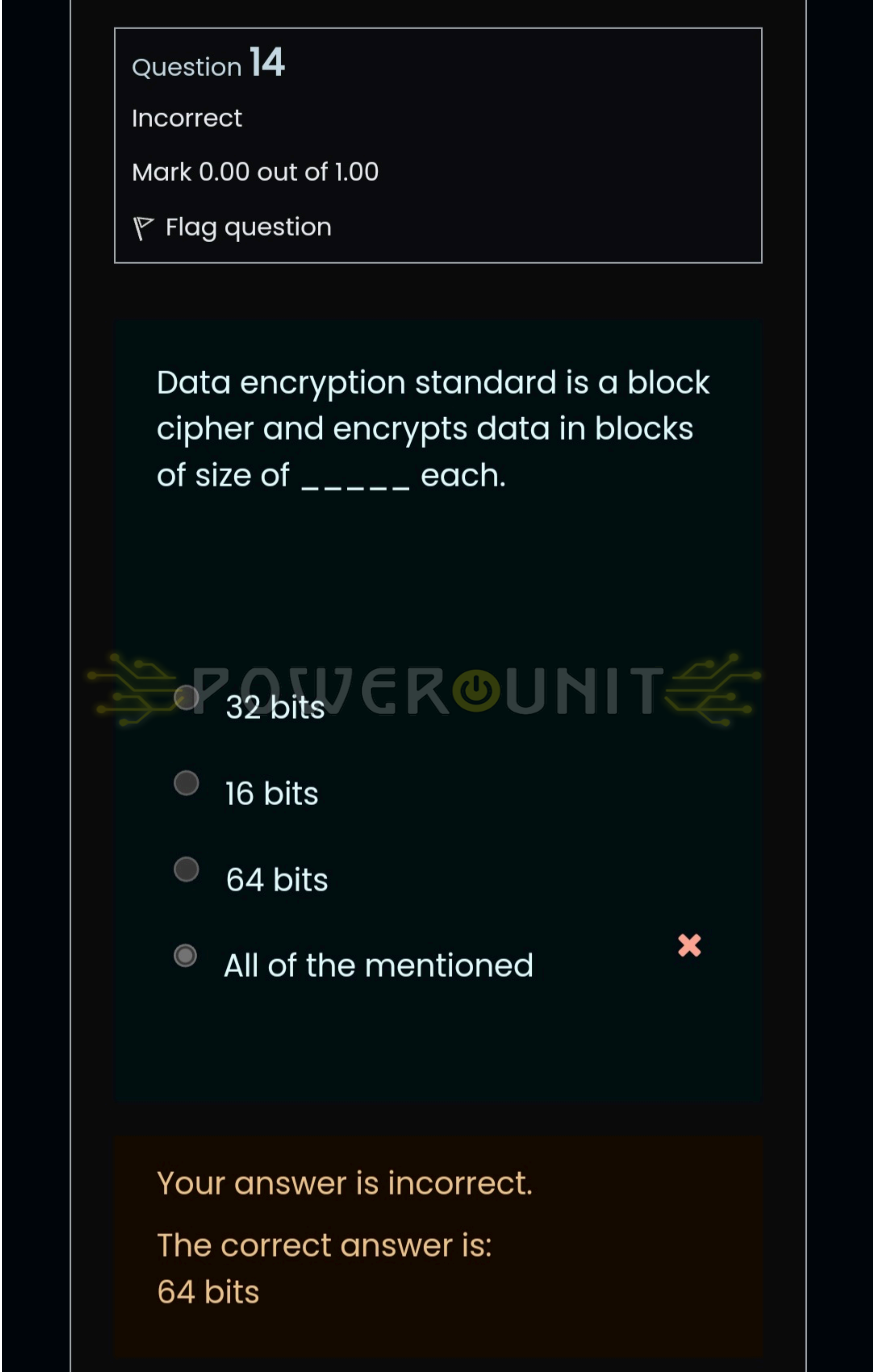
○ 9 ; the last

○ 8 ; the first and last

Your answer is incorrect.

The correct answer is:

9 ; the last



Question **14**

Incorrect

Mark 0.00 out of 1.00

Flag question

Data encryption standard is a block cipher and encrypts data in blocks of size of _____ each.

○ 32 bits

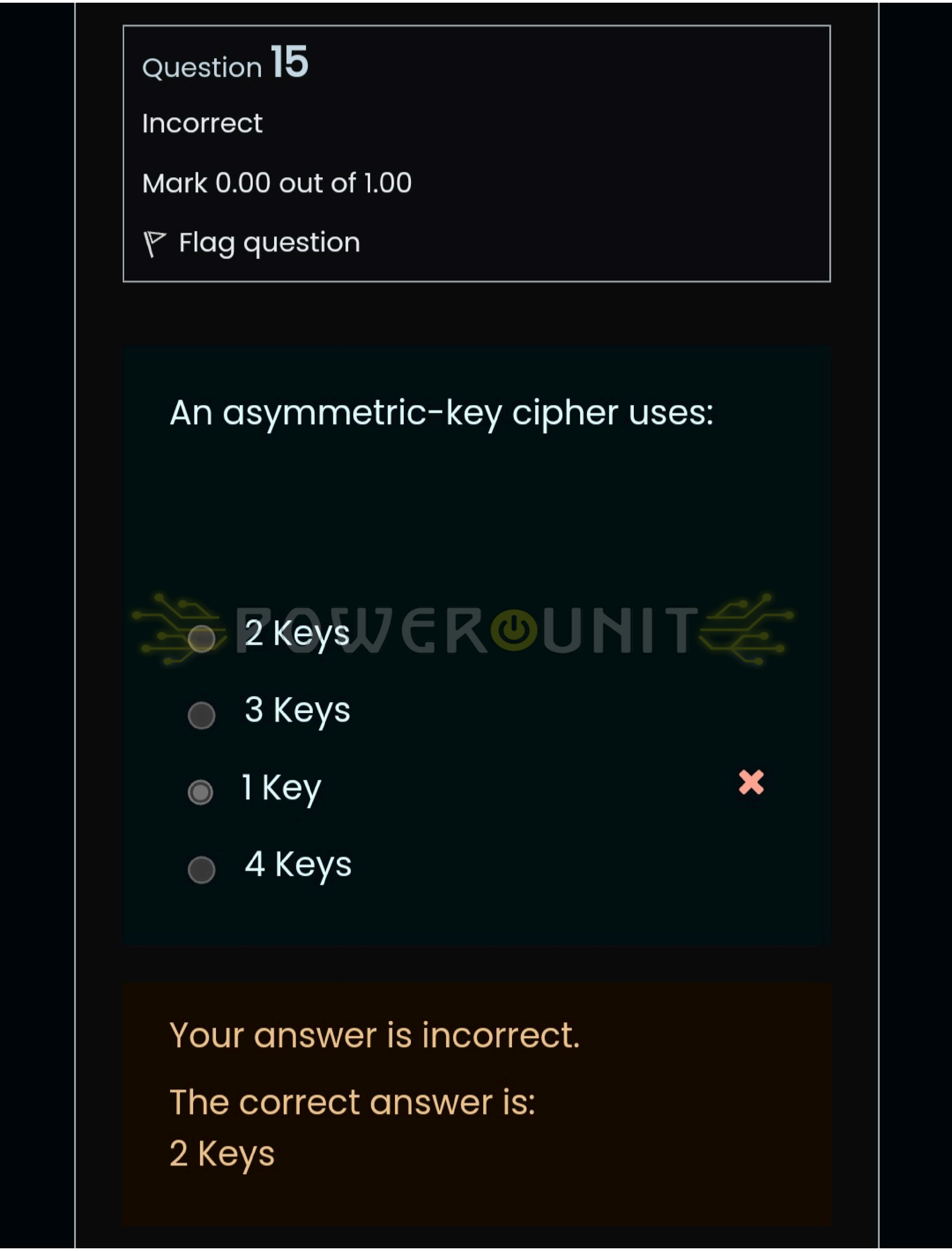
○ 16 bits

○ 64 bits

● All of the mentioned ✗

Your answer is incorrect.

The correct answer is:
64 bits



Question 15

Incorrect

Mark 0.00 out of 1.00

Flag question

An asymmetric-key cipher uses:

○ 2 Keys

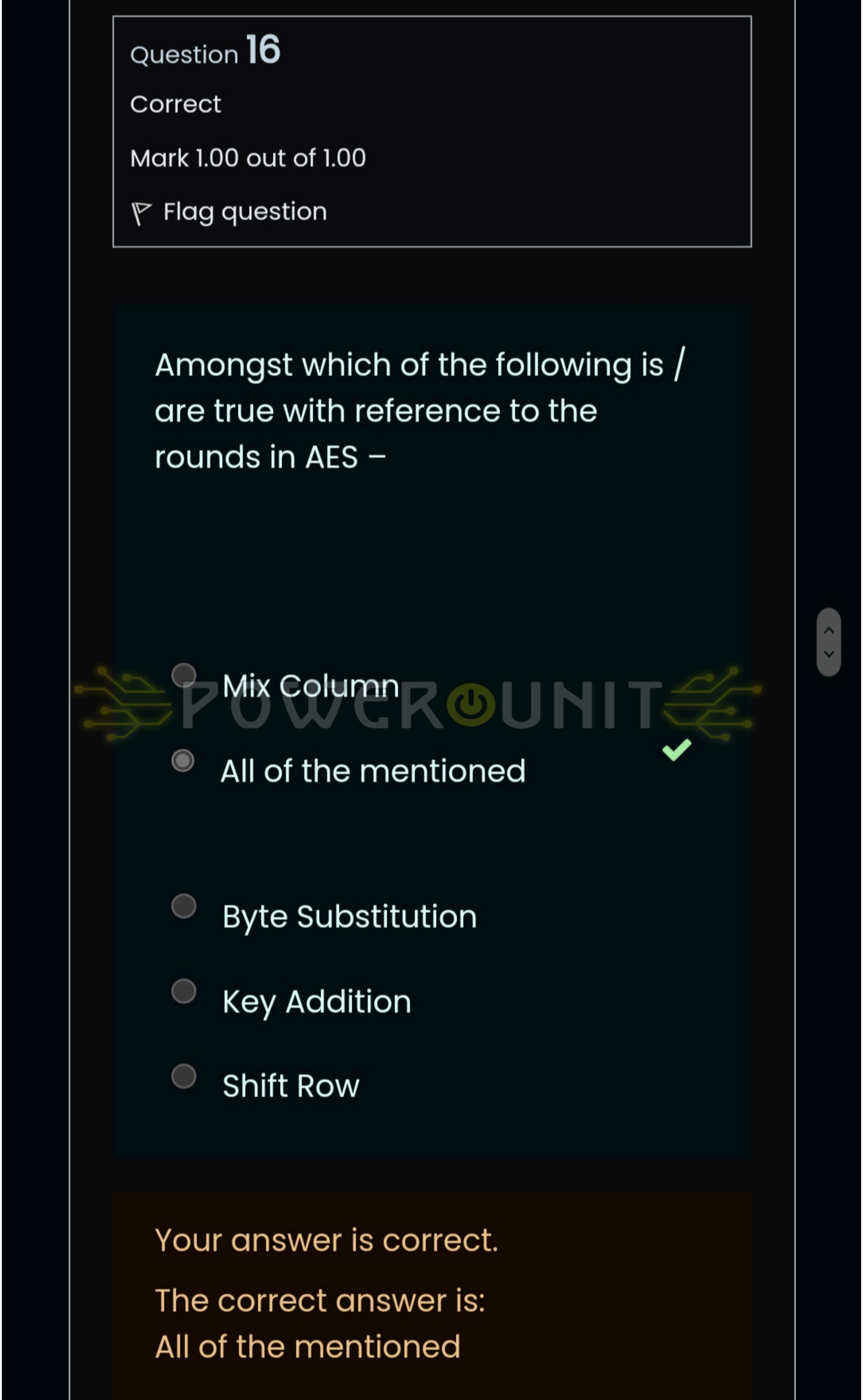
○ 3 Keys

● 1 Key ✖

○ 4 Keys

Your answer is incorrect.

The correct answer is:
2 Keys



Question 16

Correct

Mark 1.00 out of 1.00

Flag question

Amongst which of the following is / are true with reference to the rounds in AES –

○ Mix Column

◉ All of the mentioned ✓

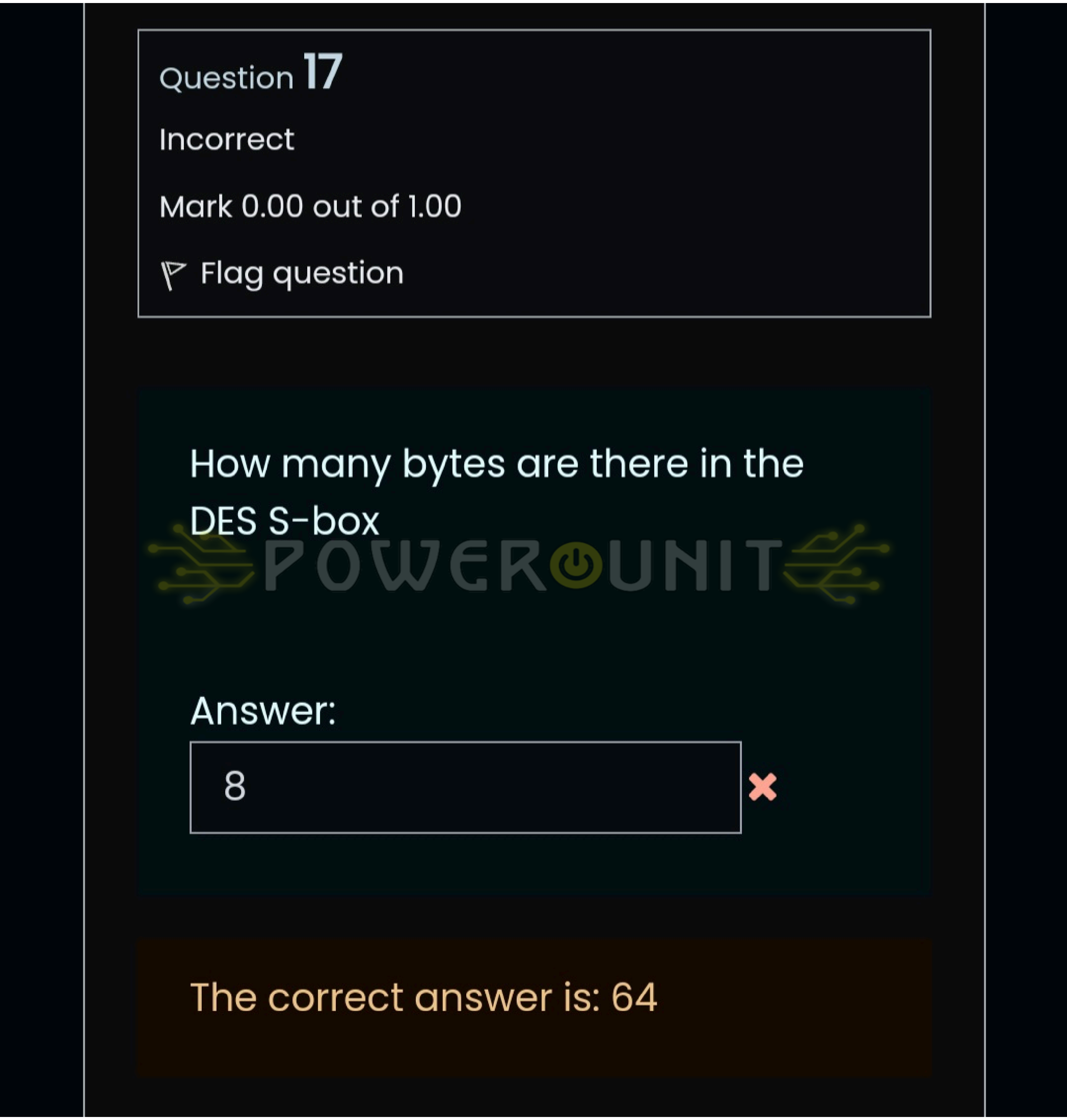
○ Byte Substitution

○ Key Addition

○ Shift Row

Your answer is correct.

The correct answer is:
All of the mentioned



Question 17

Incorrect

Mark 0.00 out of 1.00

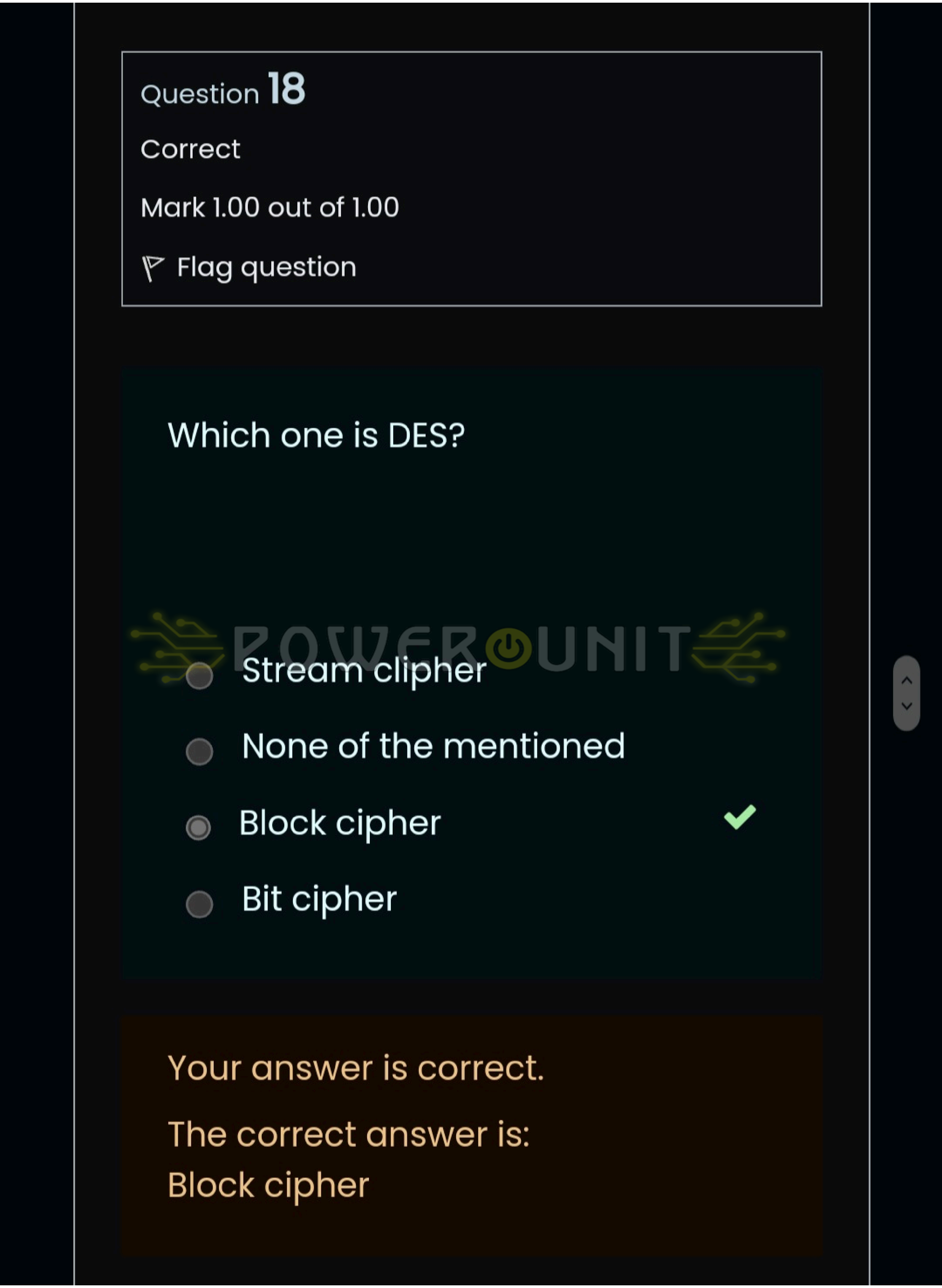
Flag question

How many bytes are there in the DES S-box

Answer:

8 ✗

The correct answer is: 64



Question 18

Correct

Mark 1.00 out of 1.00

Flag question

Which one is DES?

○ Stream clipher

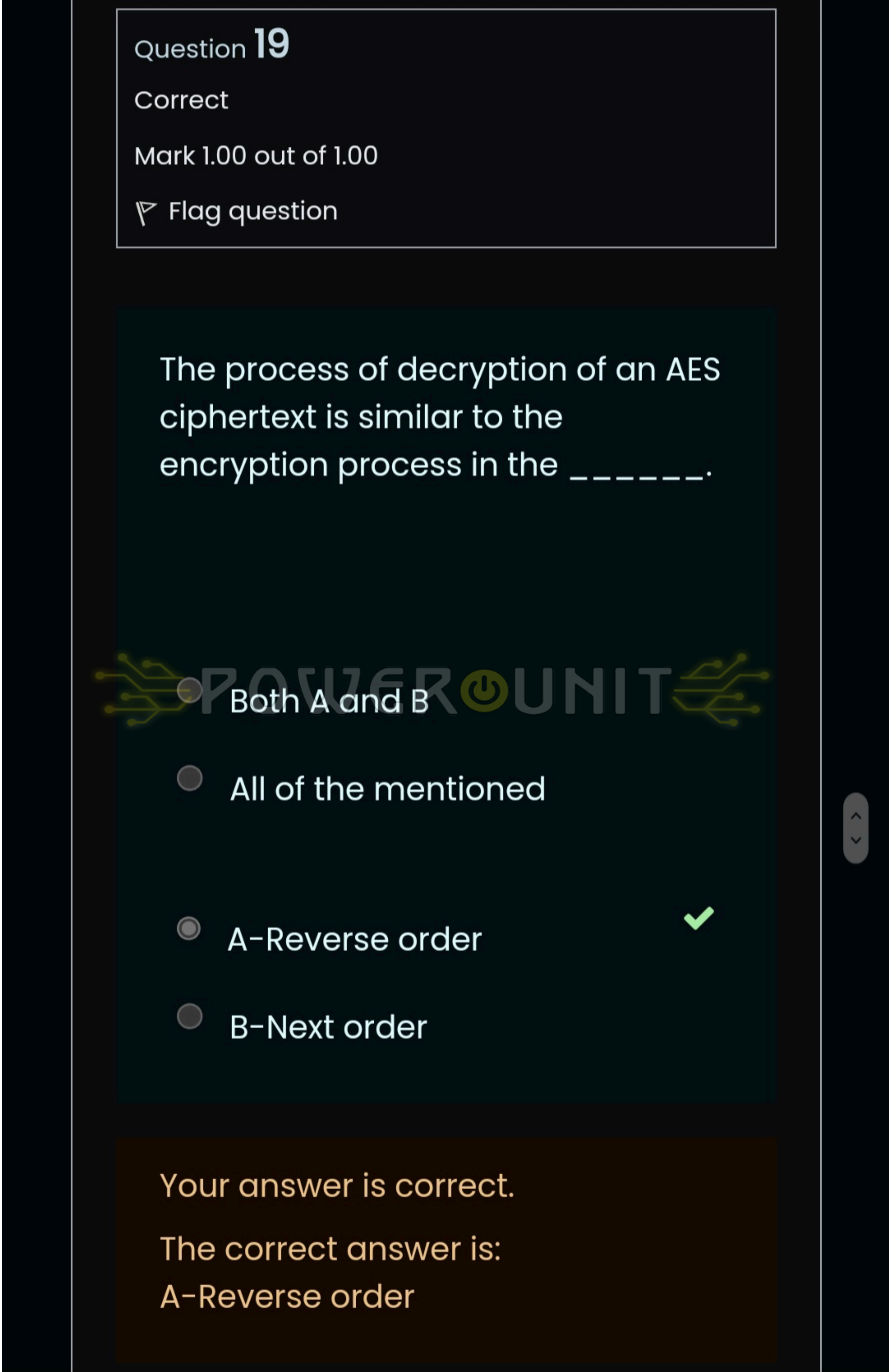
○ None of the mentioned

● Block cipher ✓

○ Bit cipher

Your answer is correct.

The correct answer is:
Block cipher



Question 19

Correct

Mark 1.00 out of 1.00

Flag question

The process of decryption of an AES ciphertext is similar to the encryption process in the _______.

○ Both A and B

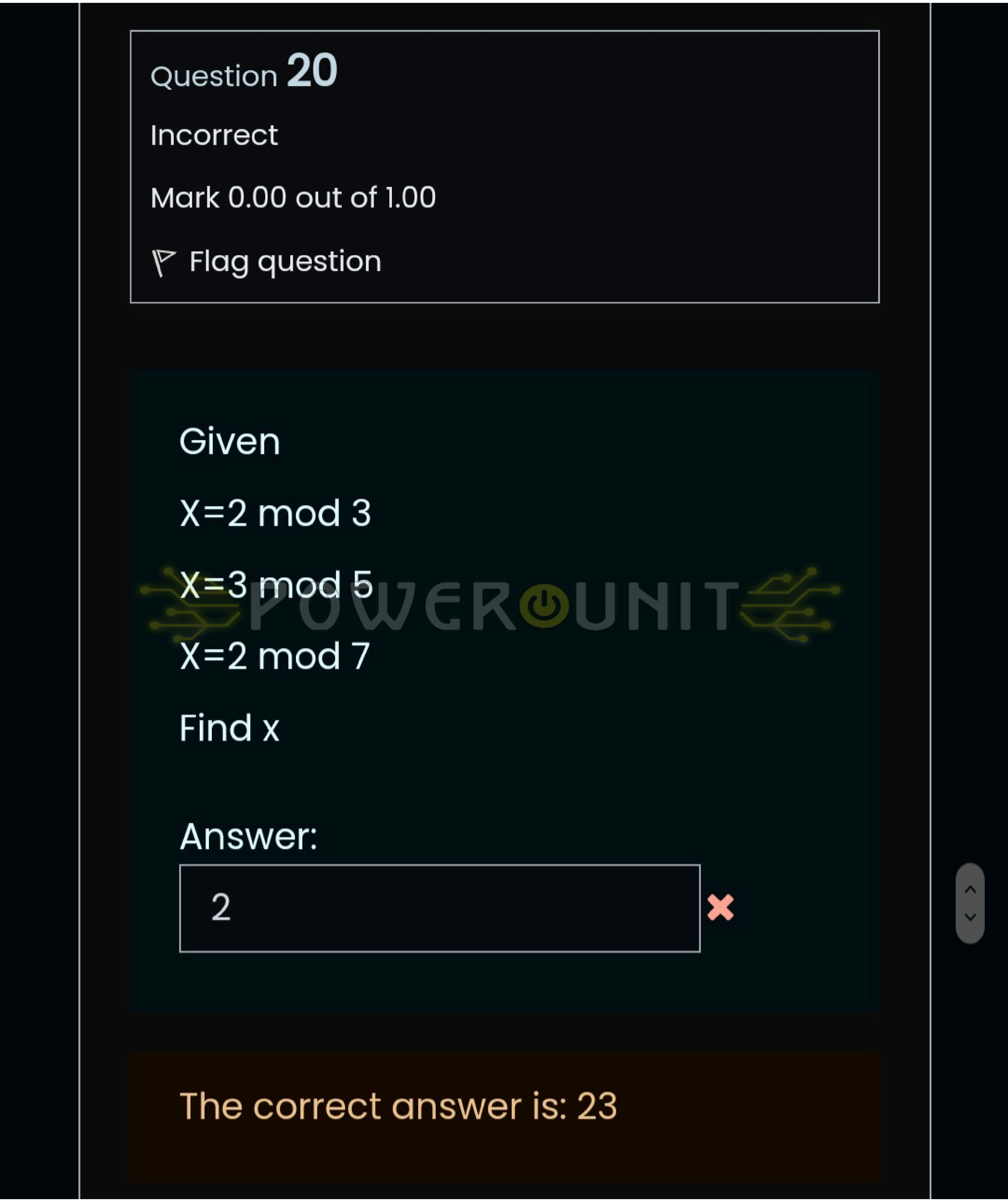
○ All of the mentioned

● A-Reverse order ✓

○ B-Next order

Your answer is correct.

The correct answer is:
A-Reverse order



Question 20

Incorrect

Mark 0.00 out of 1.00

Flag question

Given

X=2 mod 3

X=3 mod 5

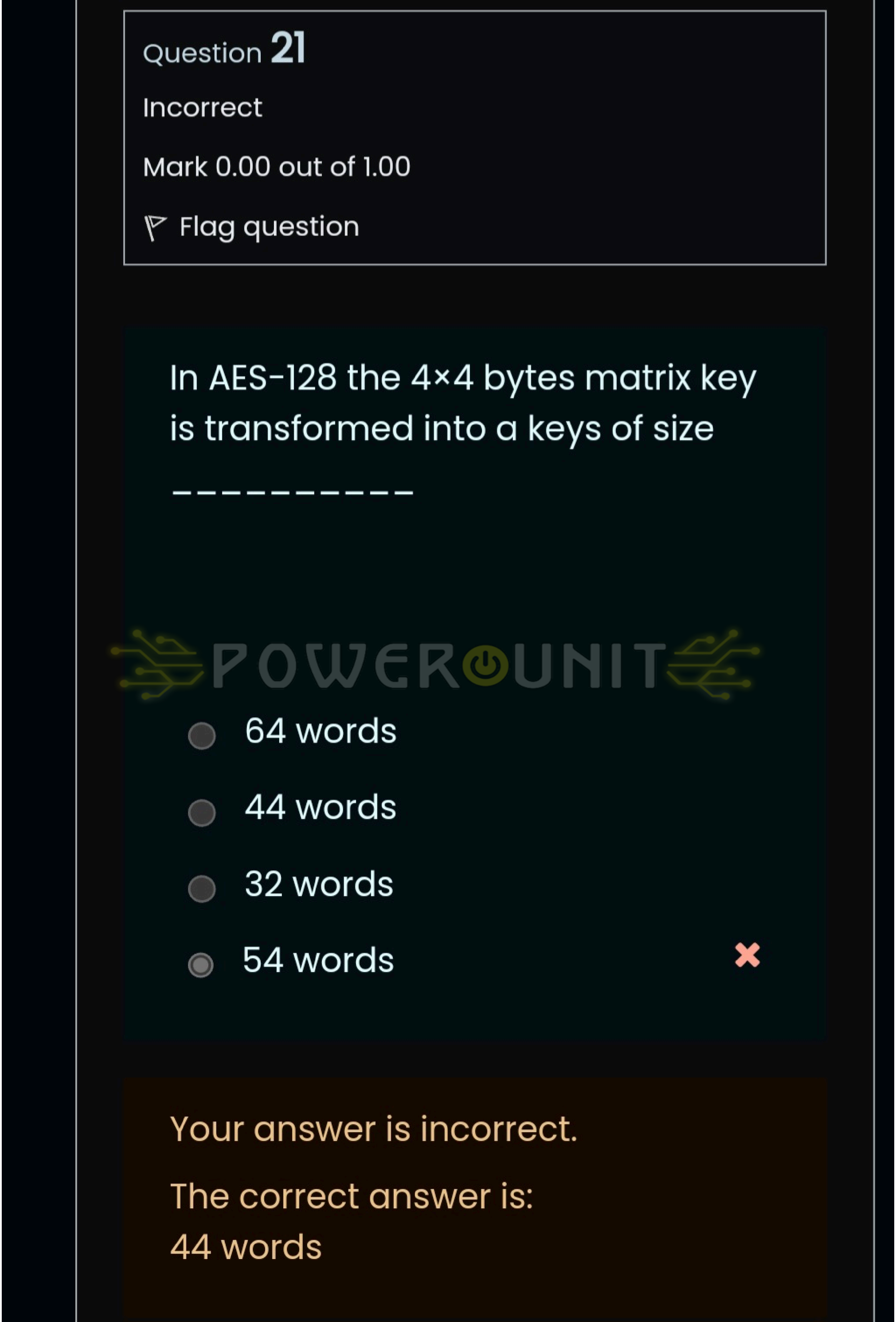
X=2 mod 7

Find x

Answer:

2 ✗

The correct answer is: 23



Question 21

Incorrect

Mark 0.00 out of 1.00

Flag question

In AES-128 the 4×4 bytes matrix key is transformed into a keys of size -----------

○ 64 words

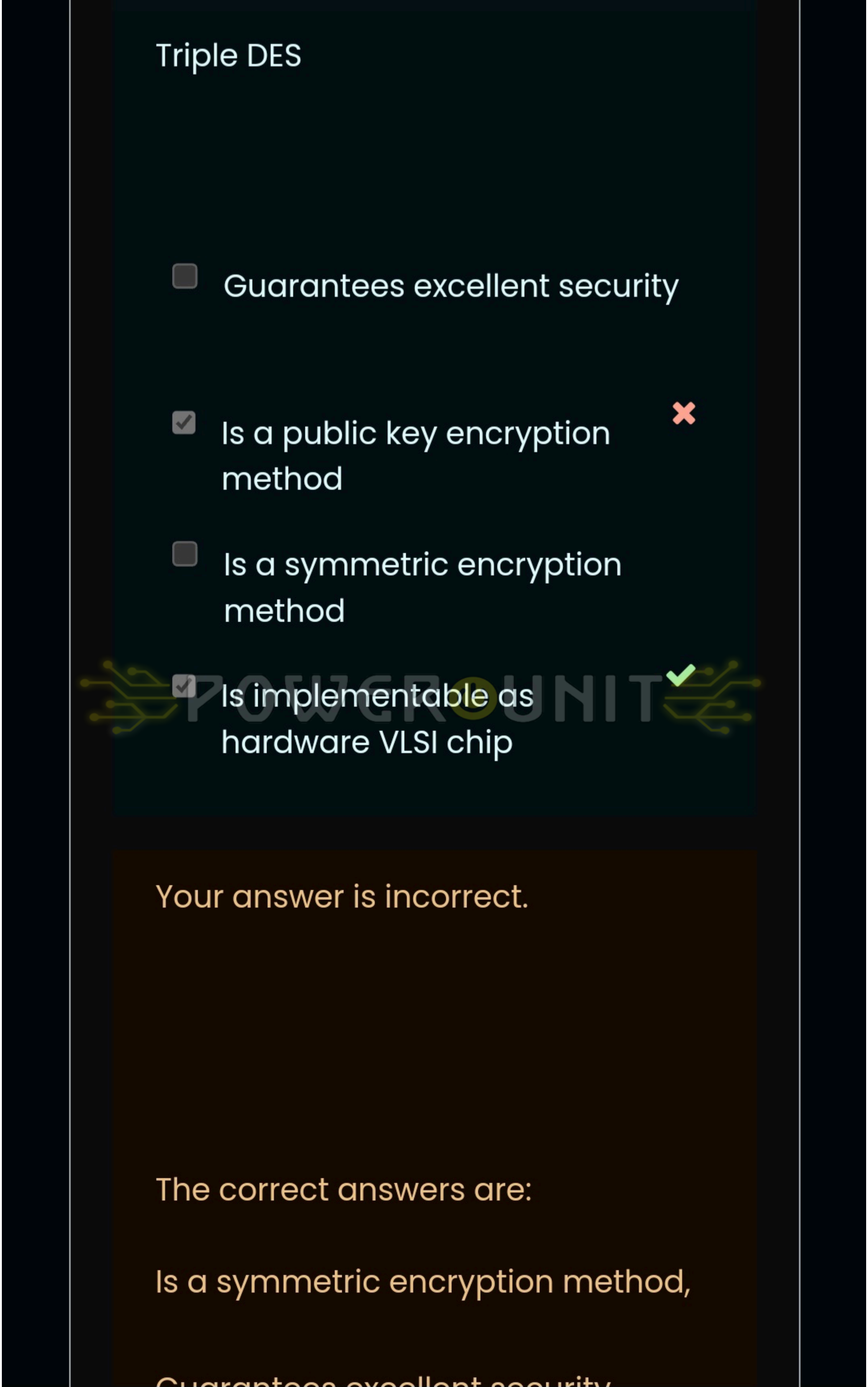
○ 44 words

○ 32 words

● 54 words ✗

Your answer is incorrect.

The correct answer is:
44 words



Triple DES

□ Guarantees excellent security

☑ Is a public key encryption method ✗

□ Is a symmetric encryption method

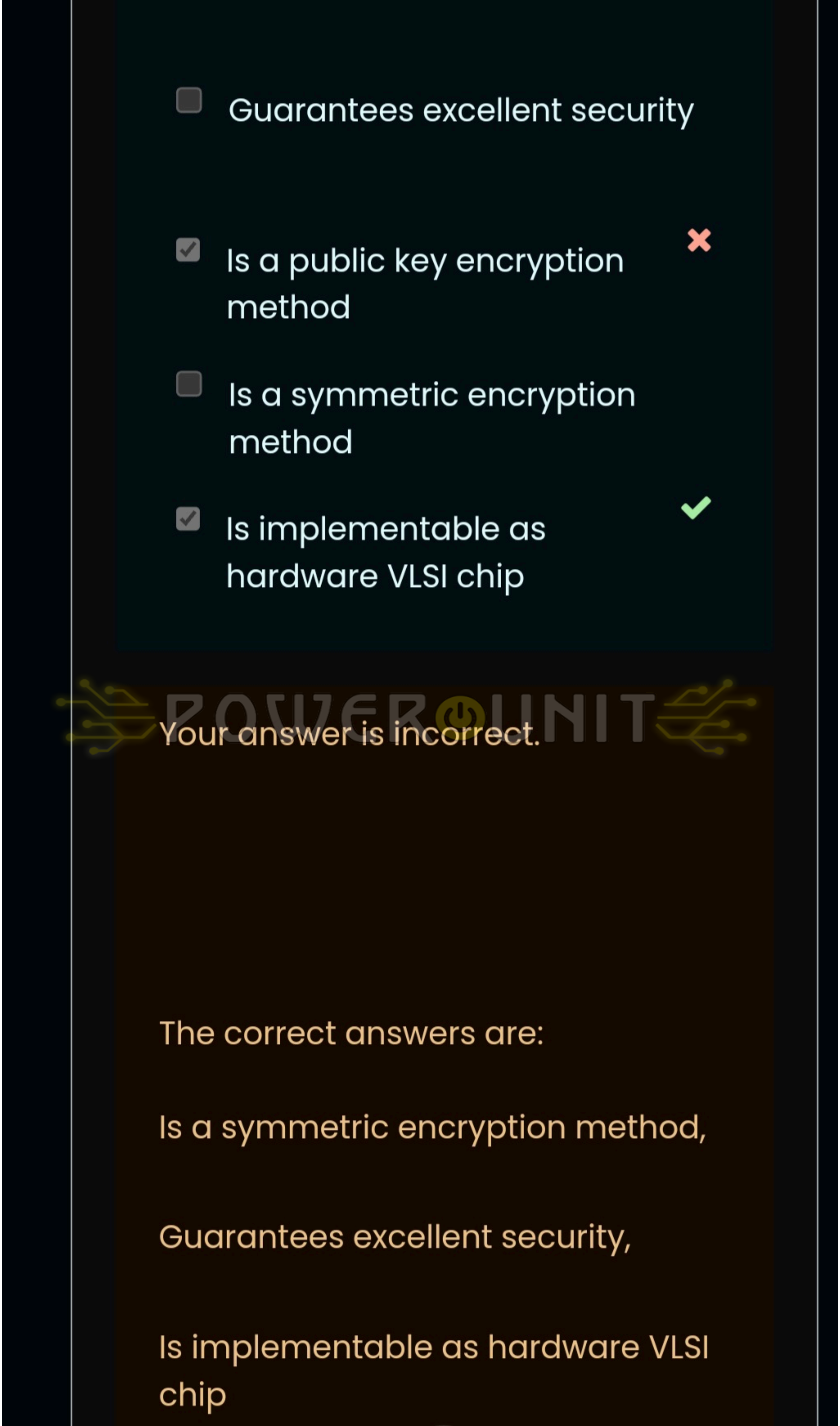
☑ Is implementable as hardware VLSI chip ✓

Your answer is incorrect.

The correct answers are:

Is a symmetric encryption method,

Guarantees excellent security



□ Guarantees excellent security

☑ Is a public key encryption method ✗

□ Is a symmetric encryption method

☑ Is implementable as hardware VLSI chip ✓

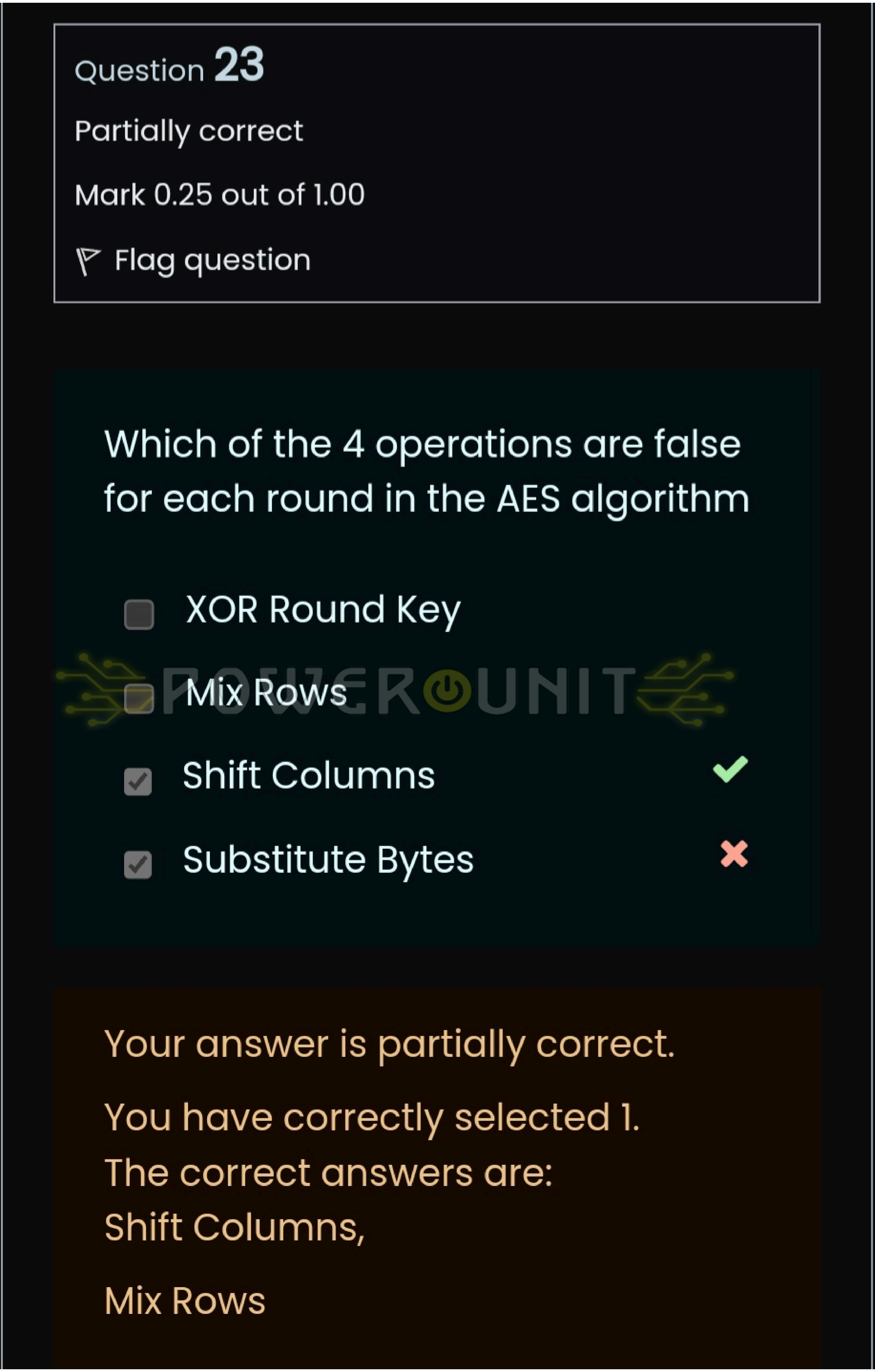
Your answer is incorrect.

The correct answers are:

Is a symmetric encryption method,

Guarantees excellent security,

Is implementable as hardware VLSI chip



Question 23

Partially correct

Mark 0.25 out of 1.00

Flag question

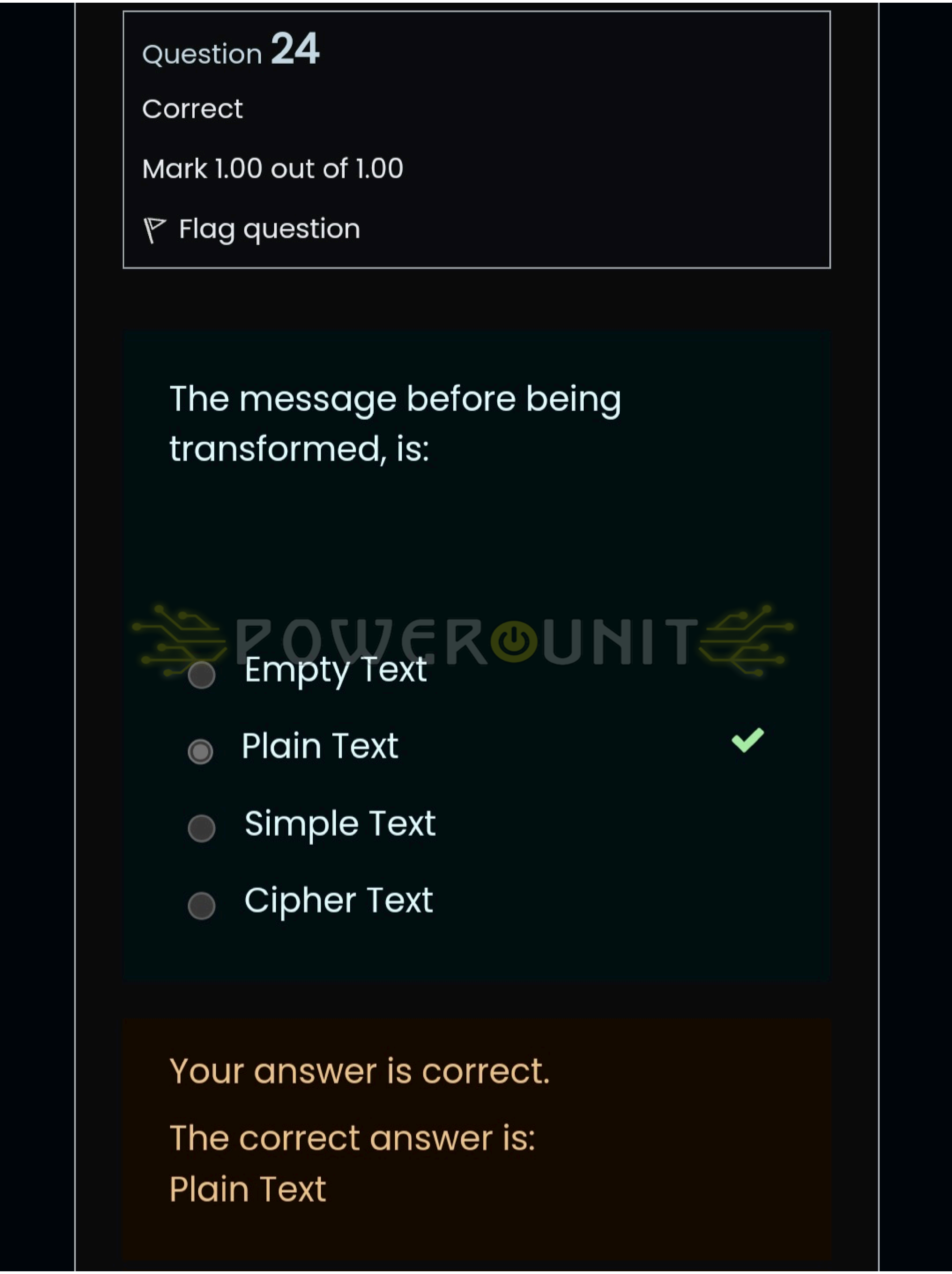
Which of the 4 operations are false for each round in the AES algorithm

- ☐ XOR Round Key
- ☐ Mix Rows
- ☑ Shift Columns ✓
- ☑ Substitute Bytes ✗

Your answer is partially correct.

You have correctly selected 1.
The correct answers are:
Shift Columns,

Mix Rows



Question 24

Correct

Mark 1.00 out of 1.00

Flag question

The message before being transformed, is:

○ Empty Text

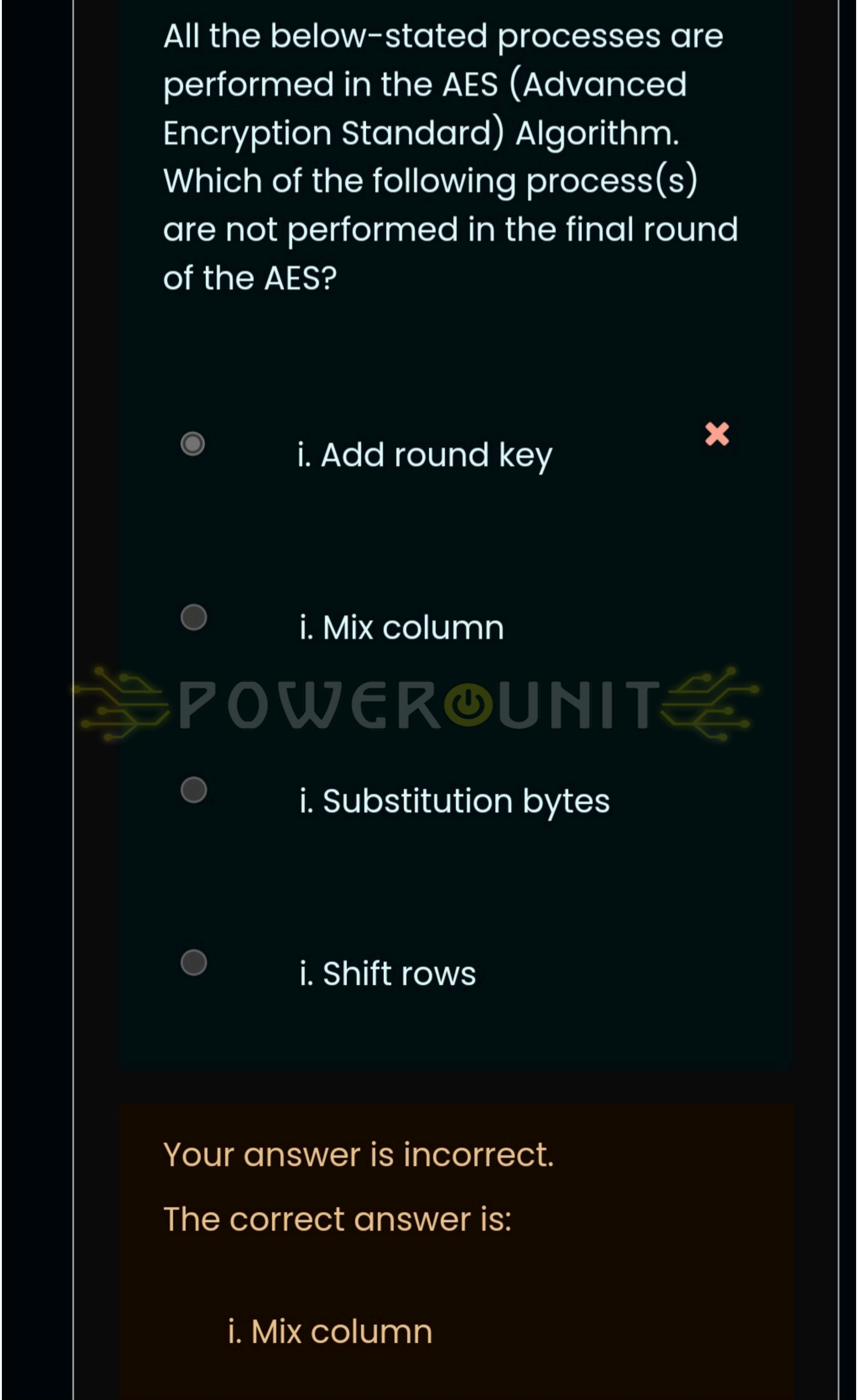
● Plain Text ✓

○ Simple Text

○ Cipher Text

Your answer is correct.

The correct answer is:
Plain Text



All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES?

● i. Add round key ✖

○ i. Mix column

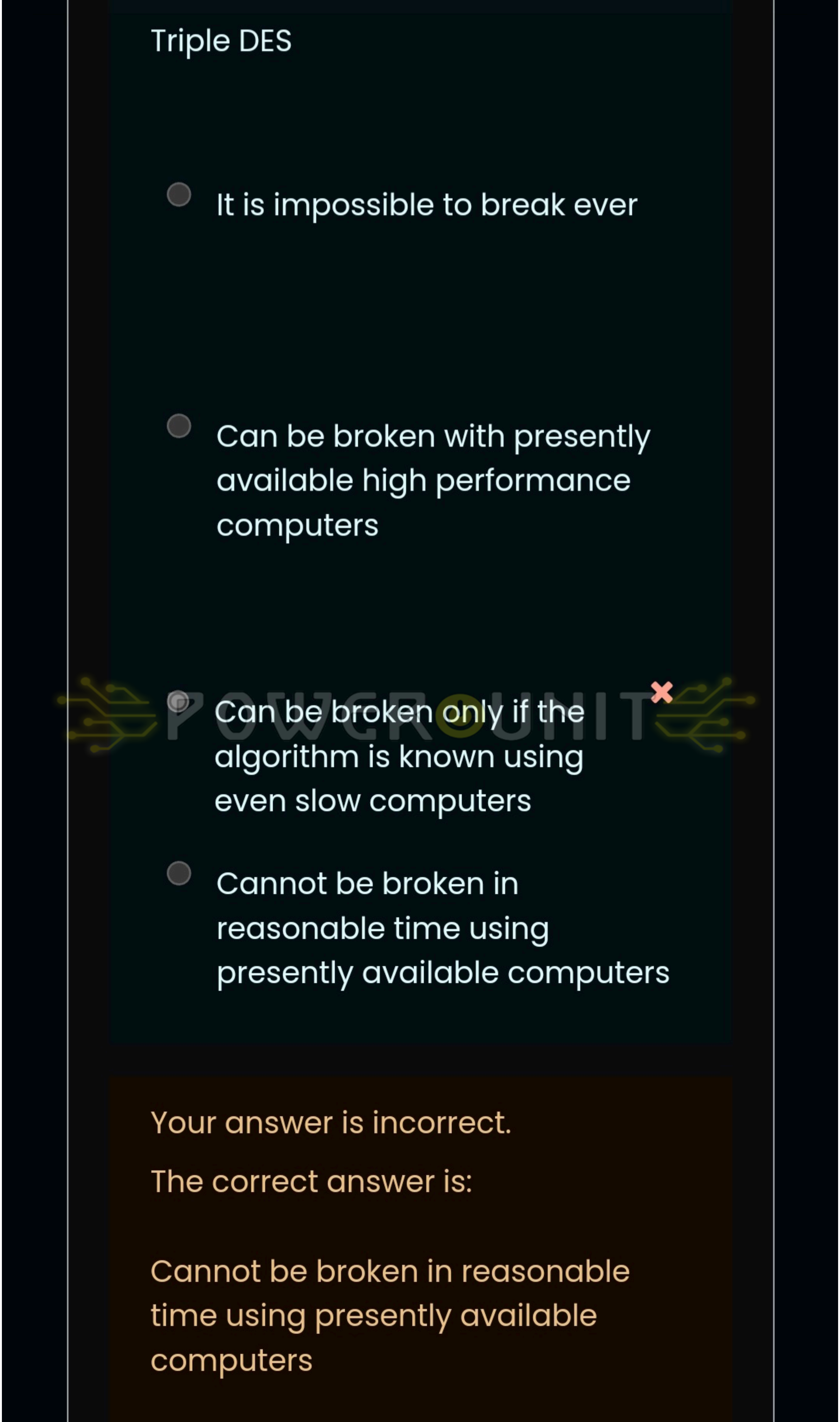
○ i. Substitution bytes

○ i. Shift rows

Your answer is incorrect.

The correct answer is:

i. Mix column



Triple DES

○ It is impossible to break ever

○ Can be broken with presently available high performance computers

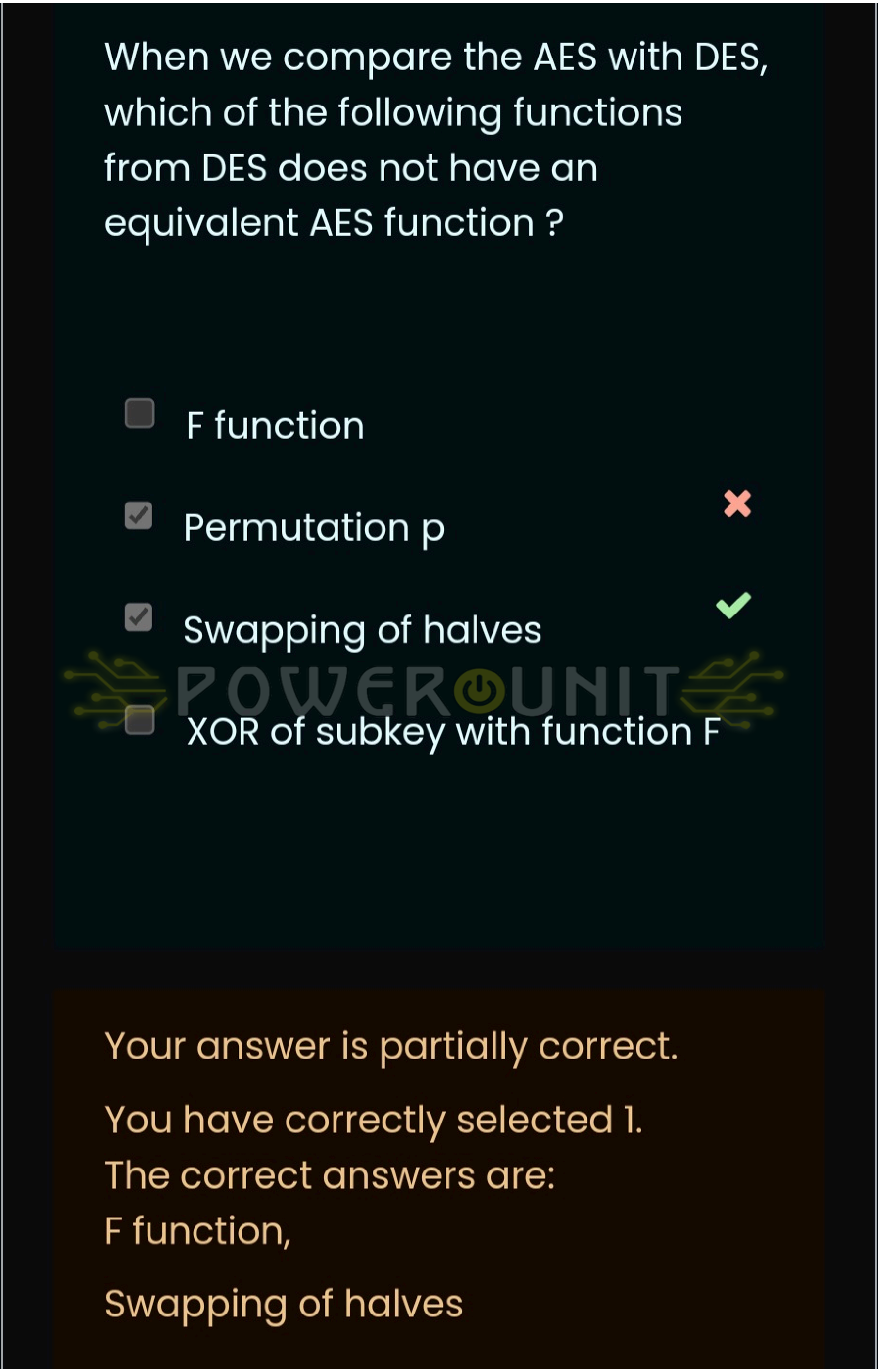
○ Can be broken only if the algorithm is known using even slow computers ✖

○ Cannot be broken in reasonable time using presently available computers

Your answer is incorrect.

The correct answer is:

Cannot be broken in reasonable time using presently available computers



When we compare the AES with DES, which of the following functions from DES does not have an equivalent AES function ?

☐ F function

☑ Permutation p ✗

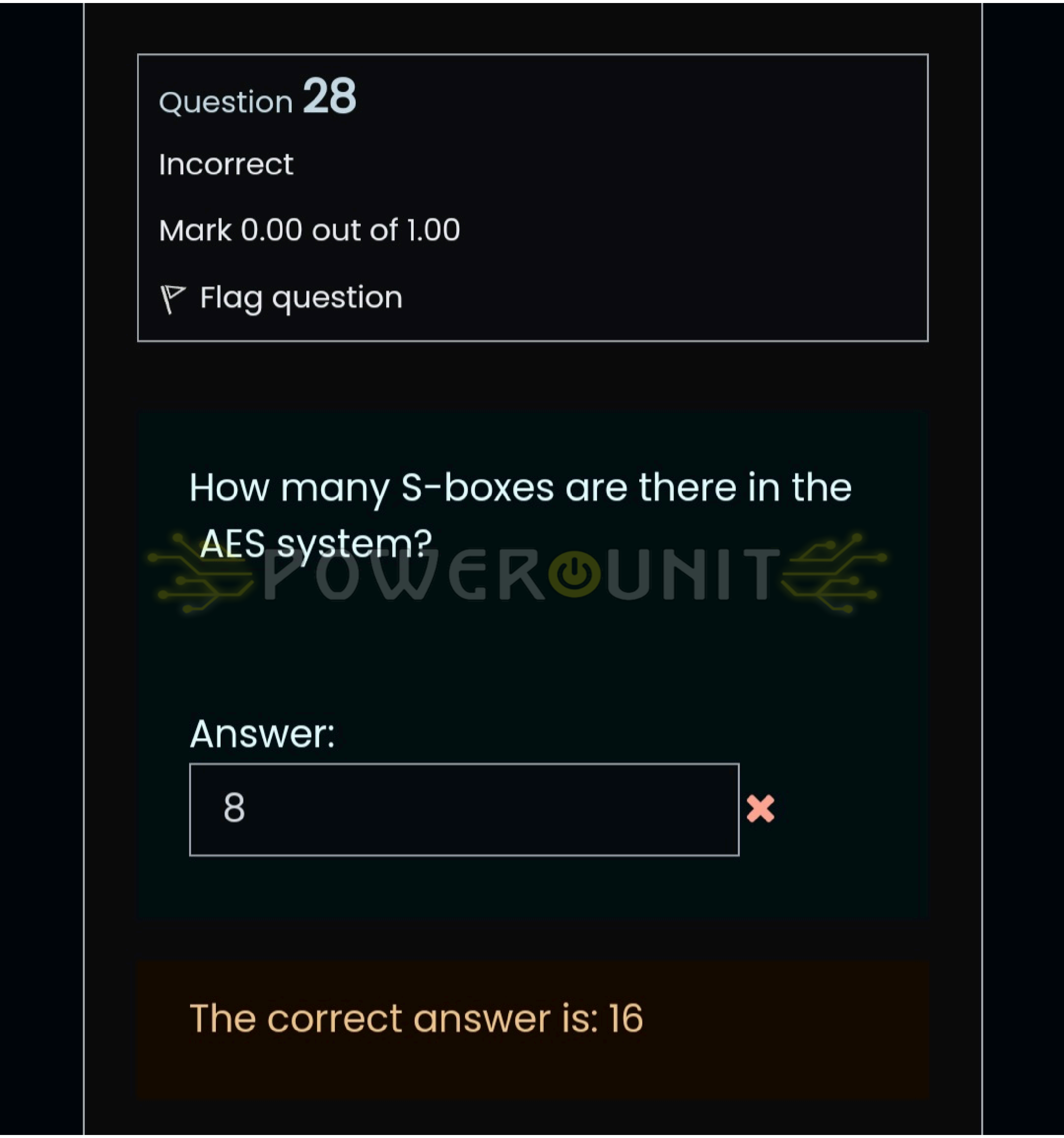
☑ Swapping of halves ✓

☐ XOR of subkey with function F

Your answer is partially correct.

You have correctly selected 1.
The correct answers are:
F function,

Swapping of halves



Question 28

Incorrect

Mark 0.00 out of 1.00

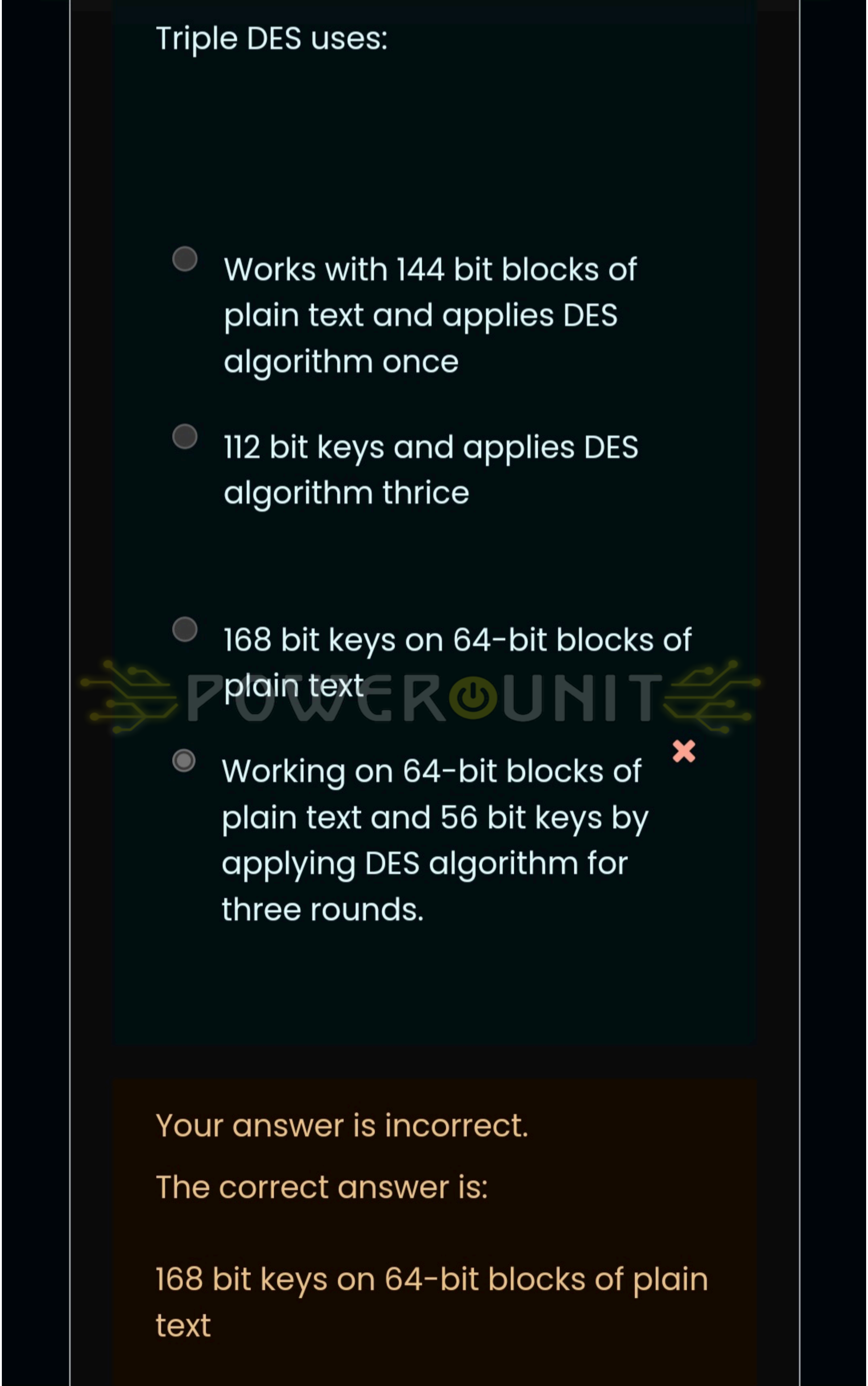
Flag question

How many S-boxes are there in the AES system?

Answer:

8 ✗

The correct answer is: 16



Triple DES uses:

○ Works with 144 bit blocks of plain text and applies DES algorithm once

○ 112 bit keys and applies DES algorithm thrice

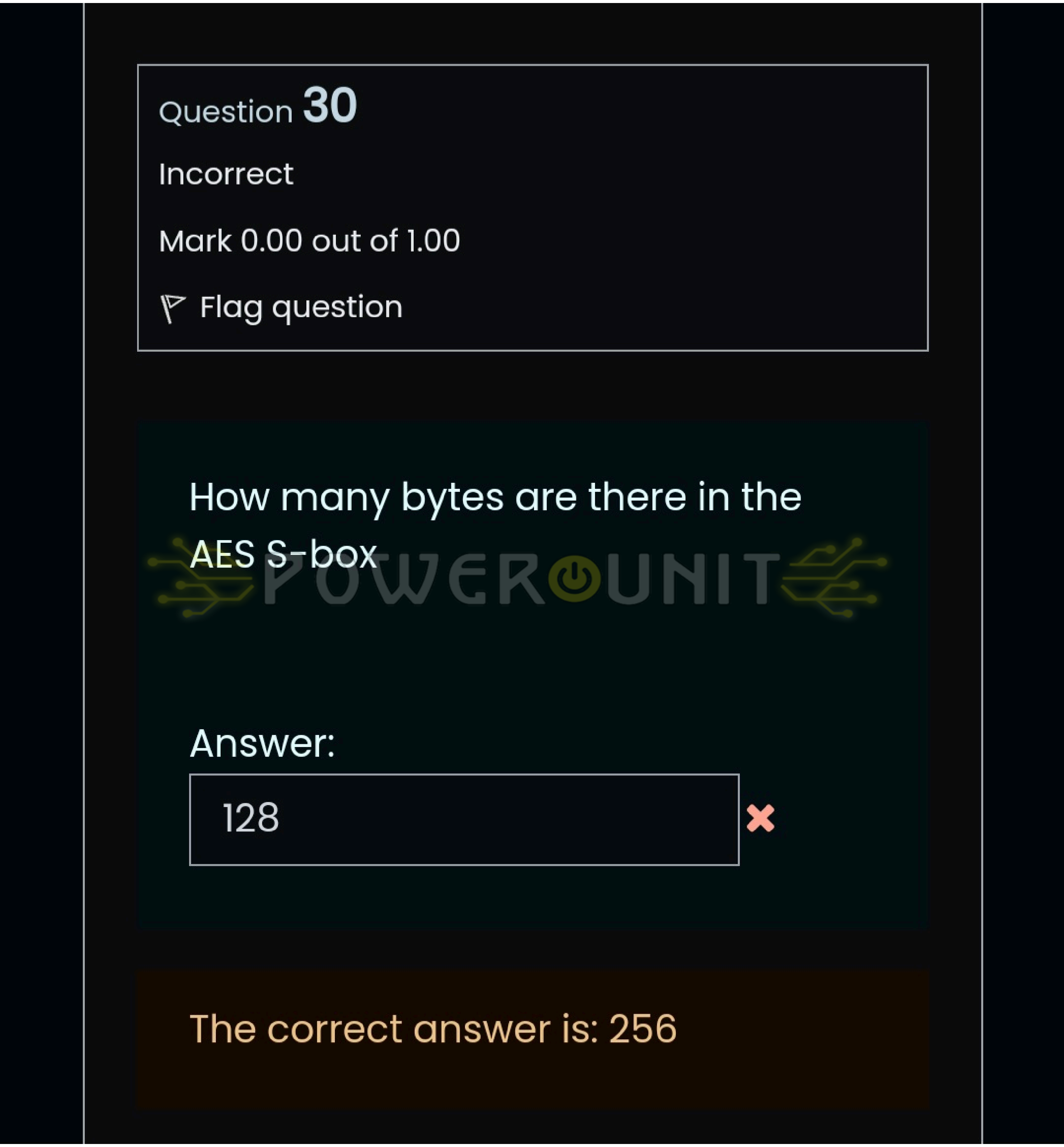
○ 168 bit keys on 64-bit blocks of plain text

◉ Working on 64-bit blocks of plain text and 56 bit keys by applying DES algorithm for three rounds. ✖

Your answer is incorrect.

The correct answer is:

168 bit keys on 64-bit blocks of plain text



Question 30

Incorrect

Mark 0.00 out of 1.00

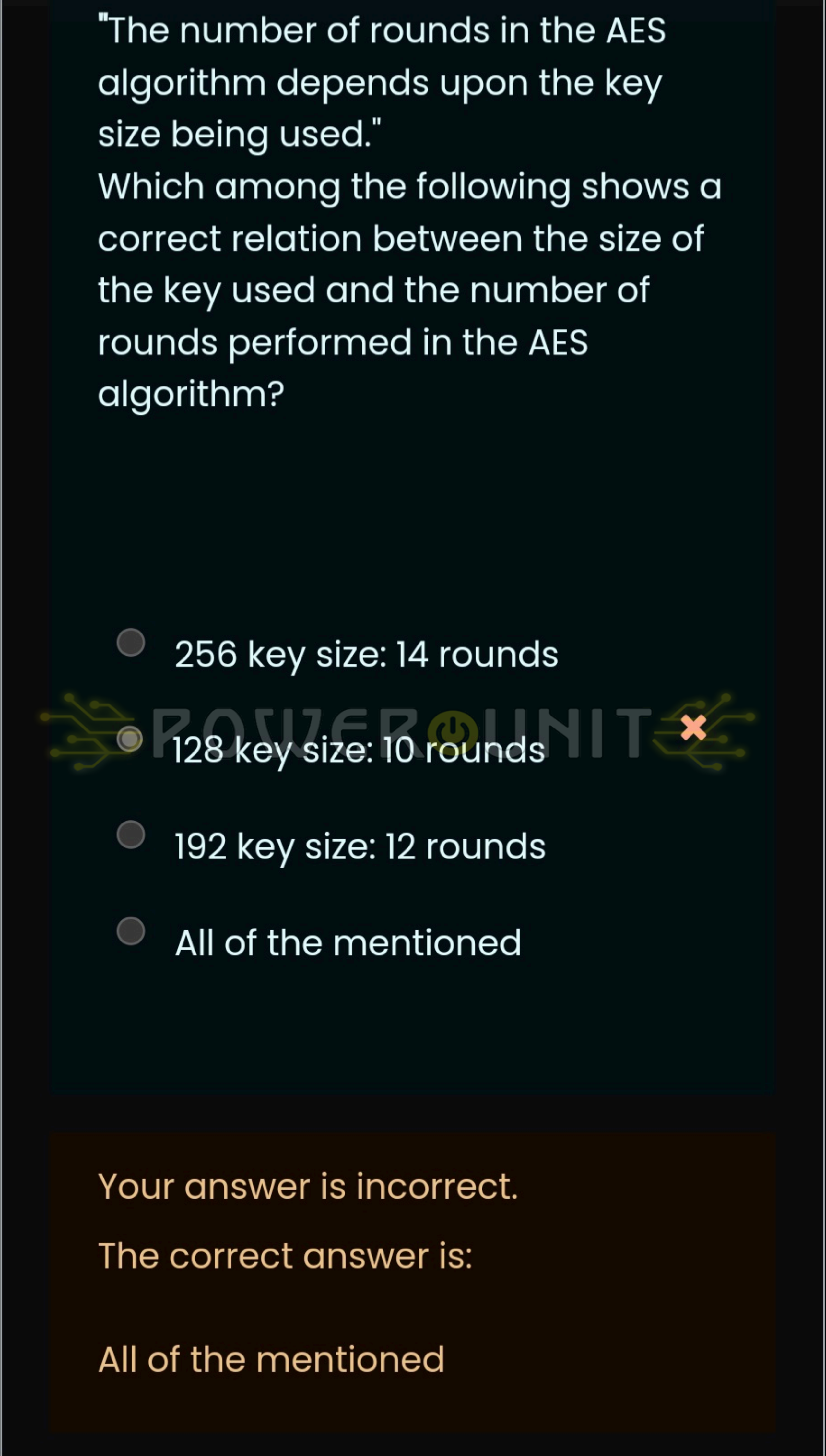
Flag question

How many bytes are there in the AES S-box

Answer:

128 ✖

The correct answer is: 256



"The number of rounds in the AES algorithm depends upon the key size being used."
Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?

○ 256 key size: 14 rounds

● 128 key size: 10 rounds ✖

○ 192 key size: 12 rounds

○ All of the mentioned

Your answer is incorrect.

The correct answer is:

All of the mentioned