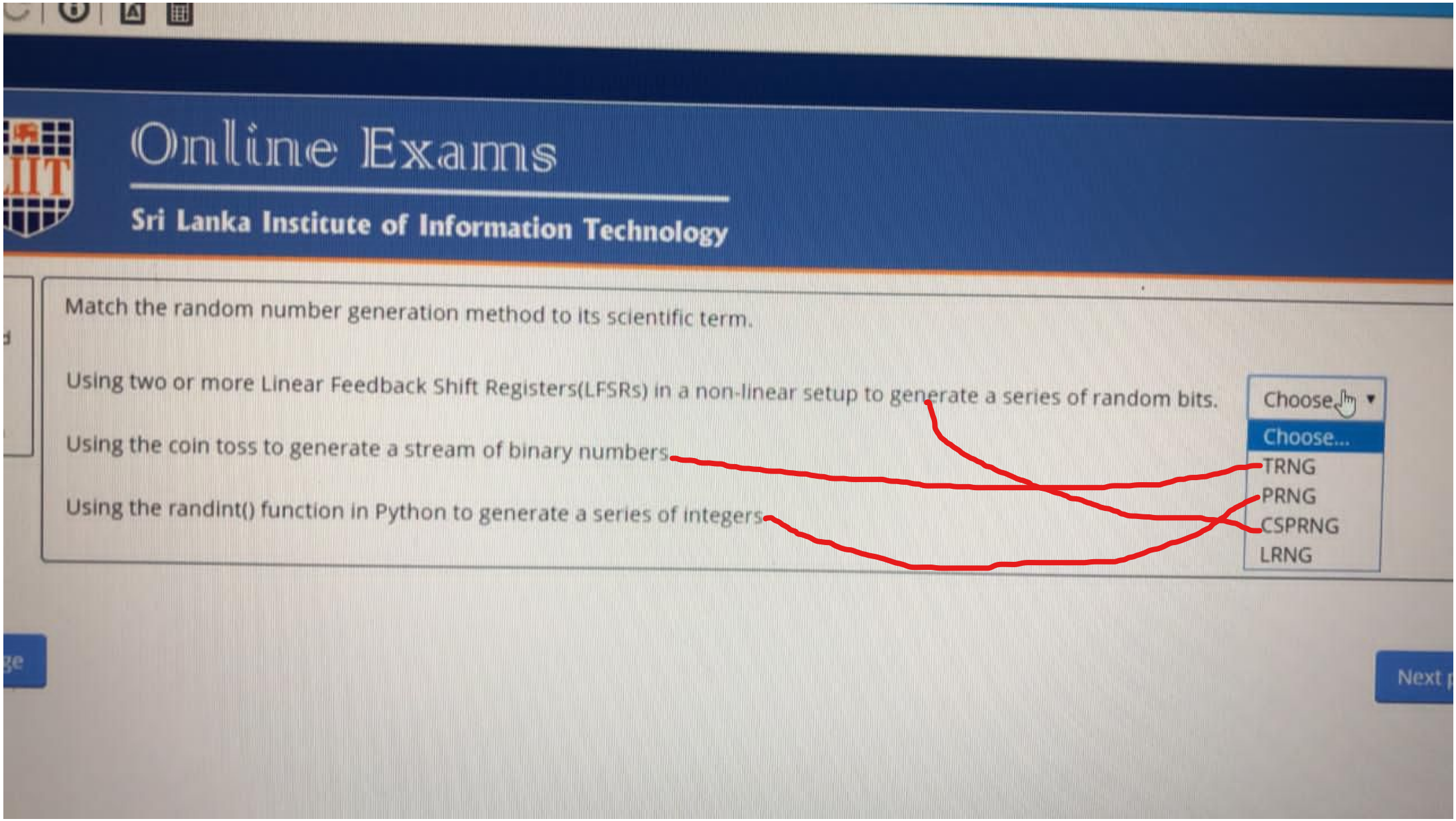
Online Exams

Sri Lanka Institute of Information Technology

Using extended Euclidean algorithm calculate the multiplicative inverse of 7 mod 26.

Answer: 15


Online Exams
Sri Lanka Institute of Information Technology
Match the random number generation method to its scientific term.
Using two or more Linear Feedback Shift Registers(LFSRs) in a non-linear setup to generate a series of random bits.
Choose...
Using the coin toss to generate a stream of binary numbers
Using the randint() function in Python to generate a series of integers
Choose...
TRNG
PRNG
CSPRNG
LRNG

Which of the following is an incorrect statement regarding Advance Encryption Standard (AES) ?

Select one:

- a. AES was chosen by the NIST in a multi-year selection process
- b. AES supports three key lengths
- c. AES is resistant to brute force attacks for the foreseeable future
- d. AES is the world standard for block encryption
- e. AES has a known weakness against differential cryptanalysis

page

Question 2

Not yet answered

Marked out of 1.00

Flag question

ORIGINAL PICTURE

ENCRYPTED PICTURE

John has encrypted an image using a block cipher. Which mode was used to encrypt the image?

Select one:

- a. Counter Mode
- b. Cipher Block Chaining Mode
- c. Electronic Code Book Mode
- d. Cipher Feedback Mode
- e. Output Feedback Mode

Online Exams

Sri Lanka Institute of Information Technology

In Output Feedback Mode (OFB) receiver does not have to use the block cipher decryption function.

Select one:

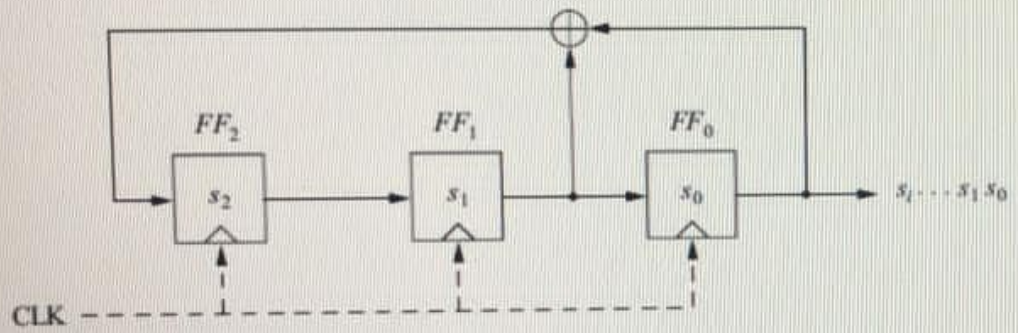
- True
- False

Online Exams

Sri Lanka Institute of Information Technology

on 1
t answered
ed out of
g question

What is the correct mathematical description of the given LFSR below?



Select one:

a. $X^3 + X + 1$

b. $X^4 + X^2 + 1$

c. $X^4 + X + 1$

d. $X^3 + X^2 + X + 1$

e. All given answers are inaccurate

Next page

Online Exams

Sri Lanka Institute of Information Technology

5

nswered

out of

question

What is the complexity of brute-forcing substitution cipher for the English alphabet?

Select one:

- a. 26 x 25
- b. 25
- c. 26!
- d. 26^{26}
- e. 26^{2}

Online Exams

Sri Lanka Institute of Information Technology

Match the correct Encryption standard to the description.

Has an input block size of 64bits and an effective key length of 112bits — Triple Data Encryption Standard (3DES)

Previously called Rijndael, eventually chosen as the world standard for block encryption — Advanced Encryption Standard (AES)

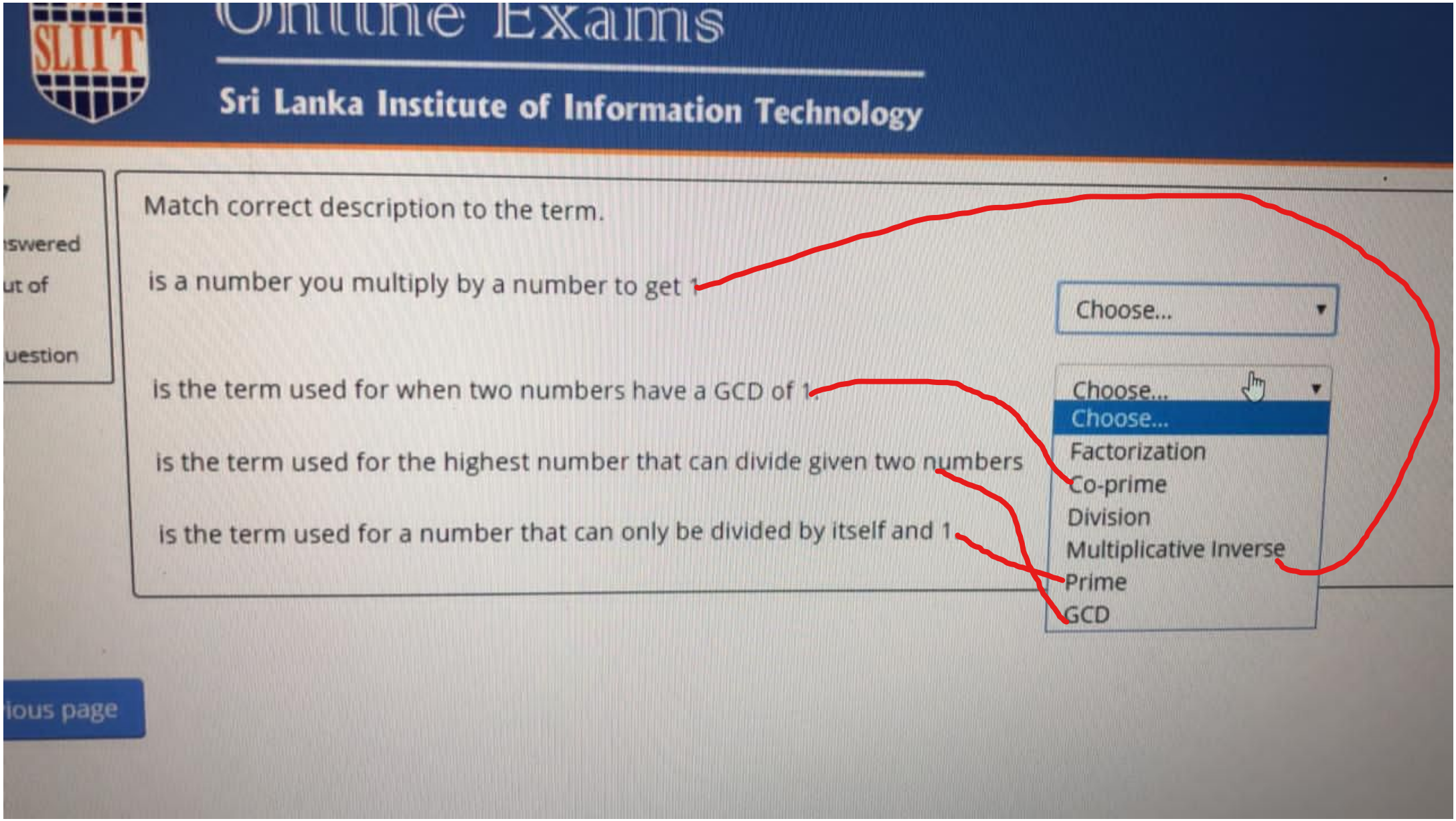
No longer used, has an input block size of 64bits and an effective key legth of 56bits — Data Encryption Standard (DES)

One of the candidate algorithms developed by IBM which was selected as a finalist in a worldwide competition. — Mars

Choose...

Choose...
Data Encryption Standard (DES)
Triple Data Encryption Standard (3DES)
Serpent
Advanced Encryption Standard (AES)
Mars
TwoFish

Next page


Online Exams
Sri Lanka Institute of Information Technology
Match correct description to the term.
is a number you multiply by a number to get 1
Choose...
is the term used for when two numbers have a GCD of 1
Choose...
is the term used for the highest number that can divide given two numbers
is the term used for a number that can only be divided by itself and 1
Choose...
Factorization
Co-prime
Division
Multiplicative Inverse
Prime
GCD

Online Exams

Sri Lanka Institute of Information Technology

What is the maximum length of random bits can be achieved with a Linear Feedback Shift Register (LFSR) with 8 registers?

Answer: 127

Online Exams

Sri Lanka Institute of Information Technology

what is the correct statement regarding 'Confusion' property in block cipher?

Select one:

- a. An operation where the relationship between plain-text and cipher-text is obscured
- b. None of the above
- c. An operation where the relationship between key and cipher-text is obscured
- d. An operation where relationship between key and plain-text is obscured
- e. An operation where the relationship between key and encryption algorithm is obscured

Online Exams

Sri Lanka Institute of Information Technology

In symmetric encryption the problem of secure communication is reduced to secure transmission and storage of the key.

Select one:

- True
- False

Online Exams

Sri Lanka Institute of Information Technology

Which of the following is not accurate regarding Random Number Generation.

Select one:

- a. PRNGs have bad cryptographic properties
- b. Coin toss can be used as a True Random Number Generation (TRNG) method
- c. Since TRNG cannot be reproduced, they cannot be used in cryptography
- d. Pseudo random number generators (PRNG) are ideal to built crypto systems

Online Exams

Sri Lanka Institute of Information Technology

Find the multiplicative inverse (a^{-1}) of a mod m, where $a * a^{-1} = 1 \bmod m$

- a = 17, m = 673

Answer: 198

page

3

swered

t of

uestion

Which of the following is not an example for 'Diffusion' property in block cipher?

Select one:

- a. DES Permutation
- b. DES S-Box
- c. DES Expansion Box
- d. AES Mix Column Layer
- e. AES Shift Row Layer

ous page

Online Exams

Sri Lanka Institute of Information Technology

Which of the following statements is an accurate definition of a 'Brute Force Attack' against an encryption algorithm?

Select one:

- a. An attacker systematically attempts all possible keys.
- b. An attacker first analyses a set of possible keys and then try the rest of the keys.
- c. An attacker analyse the cipher texts to derive few possible keys.
- d. An attacker systematically attempts selected set of keys.
- e. An attacker analyse known plain texts to derive few possible keys.

Sri Lanka Institute of Information Technology

-14 mod 6

Answer: 4

Online Exams

Sri Lanka Institute of Information Technology

What is the maximum length of random bits can be achieved with a Linear Feedback Shift Register (LFSR) with 11 registers?

Answer: 2047

Online Exams

Sri Lanka Institute of Information Technology

Which of the following is an accurate statement regarding Kerckoff's Principle?

Select one:

- a. A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the decryption algorithm.
- b. A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the encryption algorithm.
- c. A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of both encryption and decryption algorithms.
- d. A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key.
- e. All given answers are inaccurate

Next page

Online Exams

Sri Lanka Institute of Information Technology

What is the correct statement regarding non-linearity of NLFSR such as Trivium?

Select one:

- a. Non-linearity is achieved using an initialization vector
- b. Non-linearity is achieved using extra number of X-OR Gates
- c. Non-linearity is achieved using pseudo random seed values
- d. Non-linearity is achieved using multiple LFSRs connected in parallel with AND Gates
- e. Non-linearity is achieved using extra number of registers

19

nswered

out of

question

Which of the following is not a correct equation for decryption?

Select one:

a. $e^{-1}_k(x)$

b. $d_k(e_k(x))$

c. $e^{-1}_k(y)$

d. All are correct

e. $d_k(y)$

Which of the following mode has the fastest encryption implementation?

Select one:

- a. Cipher Block Chaining mode(CBC)
- b. Cipher Feedback mode(CFB)
- c. Counter mode(CTR)
- d. Block mode(BM)
- e. Output Feedback mode(OFB)

Online Exams

Sri Lanka Institute of Information Technology

In Affine cipher, the key consists of two parts k = (a,b). Which of the following is a suitable 'a,b' pair? Affine cipher encryption and decryption is given below

Let k, x, y ε {0,1, …, 25}

- Encryption: $y = e_K(x) \equiv a\,x + b \bmod 26$
- Decryption: $x = d_K(x) \equiv a^{-1}(y - b) \bmod 26$

Select one:

- a. a = 13, b = 7
- b. a = 8, b = 9
- c. a = 4, b = 15
- d. a = 11, b = 3
- e. None of the above

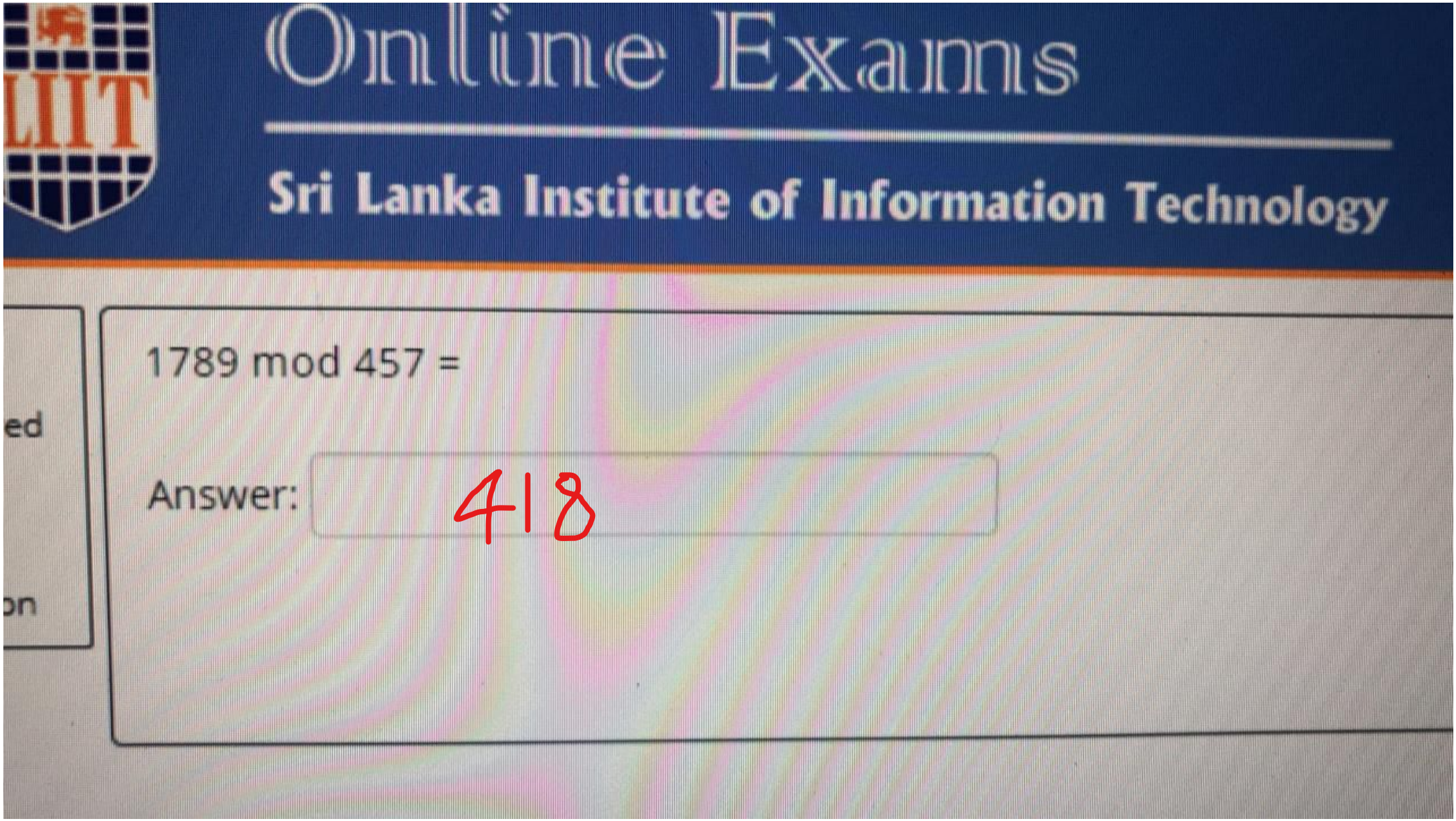
Next page

Sri Lanka Institute of Information Technology

Which of the following is not a reason to use X-OR as an encryption function in stream ciphers?

Select one:

- a. Ease of implementation
- b. Encryption and Decryption both achieved by the same function
- c. Ability to use in an asynchronous setup
- d. Efficiency
- e. 50% chance of output being '1' or '0'


Online Exams
Sri Lanka Institute of Information Technology
1789 mod 457 =
Answer:
418

Online Exams

Sri Lanka Institute of Information Technology

Initialization Vector (IV) is a secret value used to start the block encryption mechanism in Cipher Block Chaining mode.

Select one:

- True
- False