EXPERIMENT-05

Aim: To understand how to Encrypt long messages using various modes of operation using AES or DES.

Roll No.	70
Name	MAYURI SHRIDATTA YERANDE
Class	D15-B
Subject	Internet Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

AIM: To understand how to Encrypt long messages using various modes of operation using AES or DES.

THEORY:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

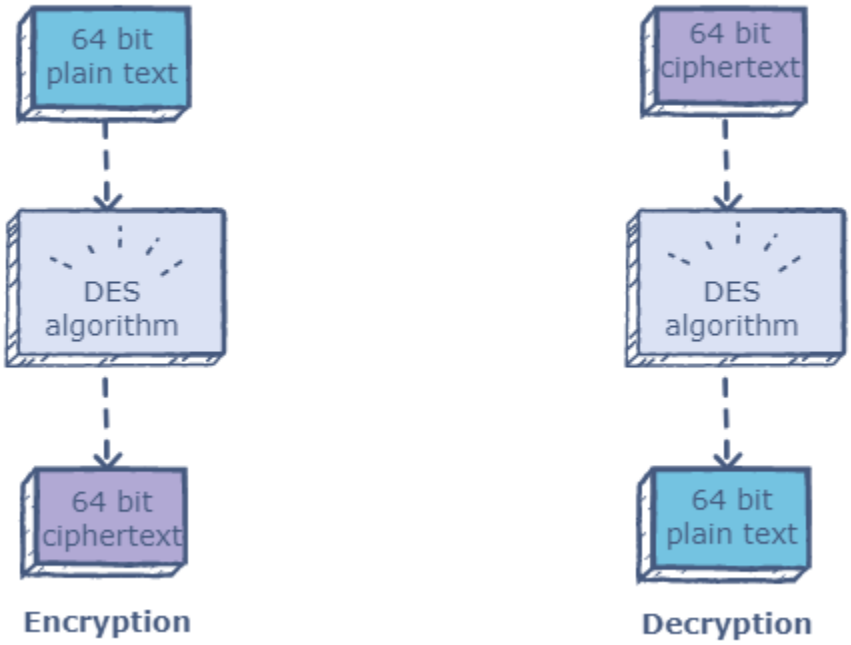
A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Data Encryption Standard (DES) is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to ciphertext using keys of 48 bits. It is a symmetric key algorithm, which means that the same key is used for encrypting

and decrypting data.

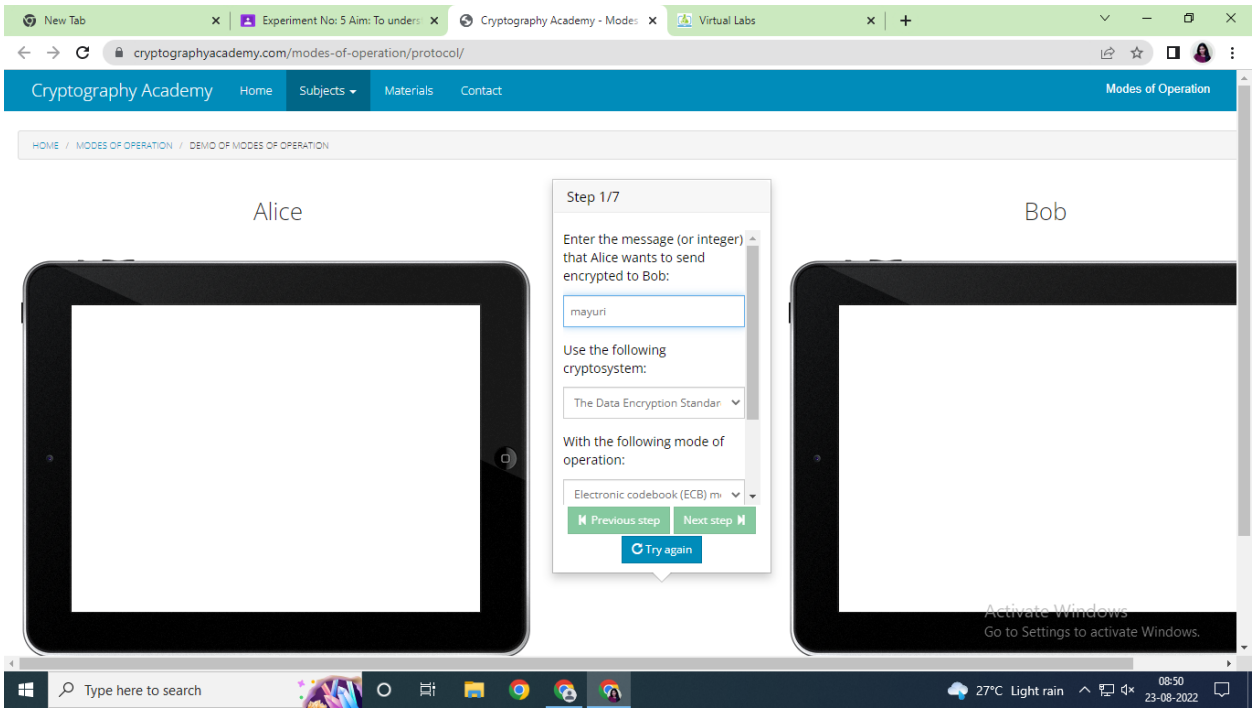


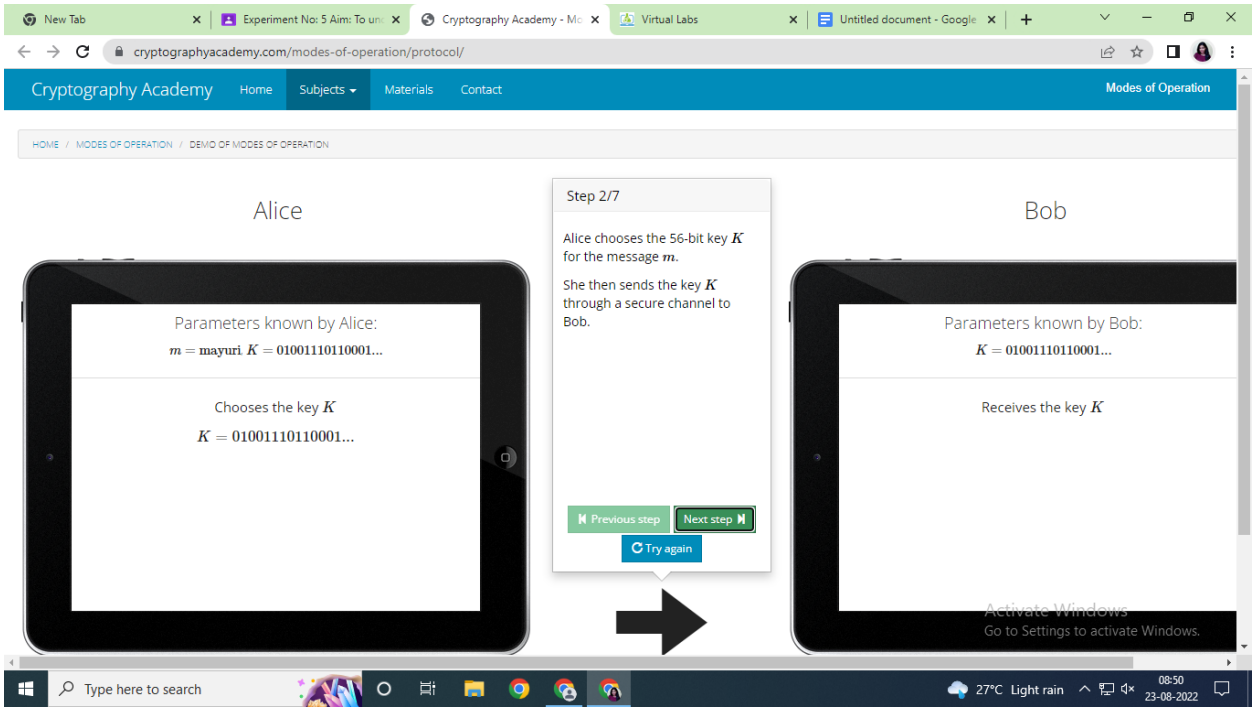
AES	DES
AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
The date of creation is 1999.	The date of creation is 1976.
Byte-Oriented.	Bit-Oriented.
Key length can be 128-bits, 192-bits, and 256-bits.	The key length is 56 bits in DES.

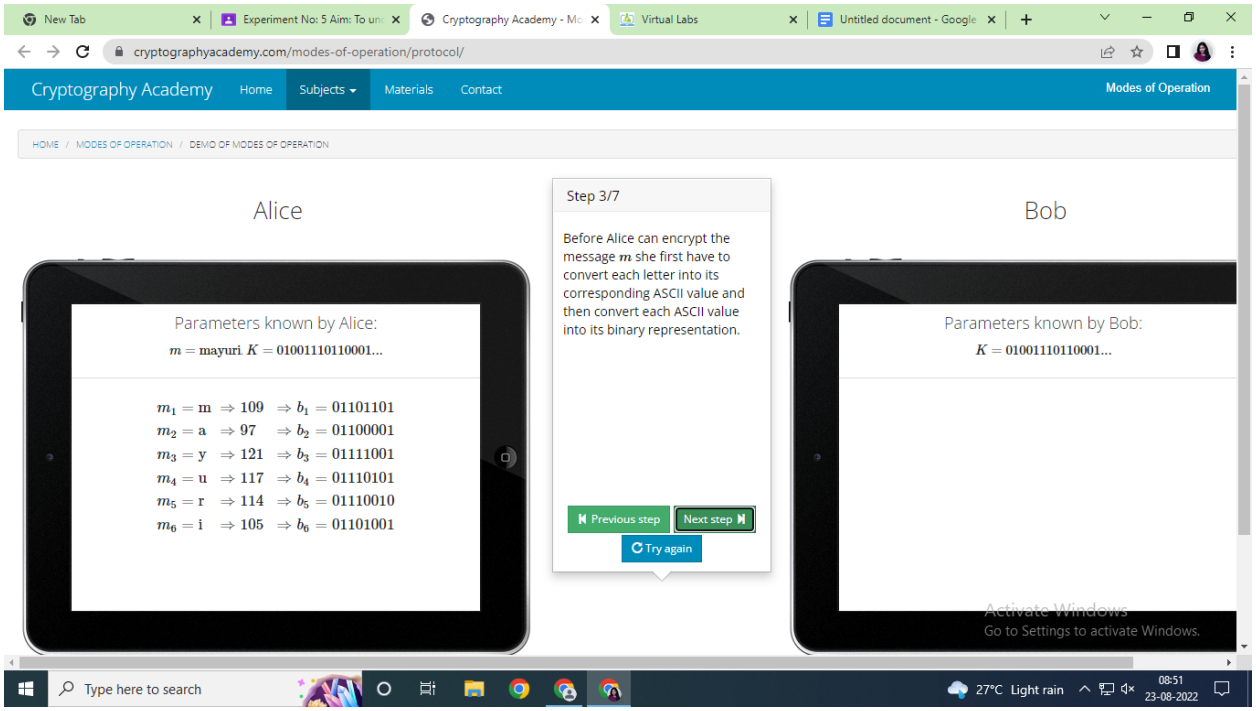
Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations
The structure is based on a substitution-permutation network.	The structure is based on a Feistel network.
The design rationale for AES is open.	The design rationale for DES is closed.
The selection process for this is secret but accepted for open public comment.	The selection process for this is secret.
AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.
AES cipher is derived from an aside-channel square cipher.	DES cipher is derived from Lucifer cipher.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.
No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attacks have better complexity than brute force but still ineffective.	Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis.

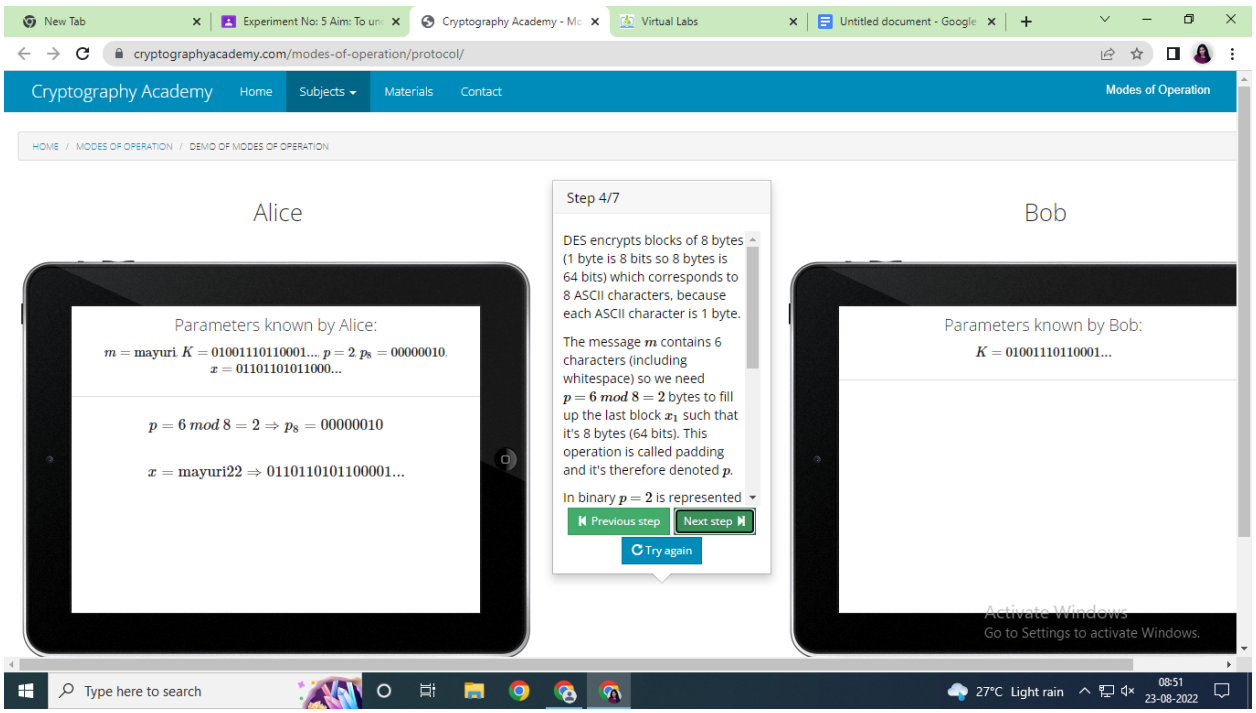
IMPLEMENTATION:

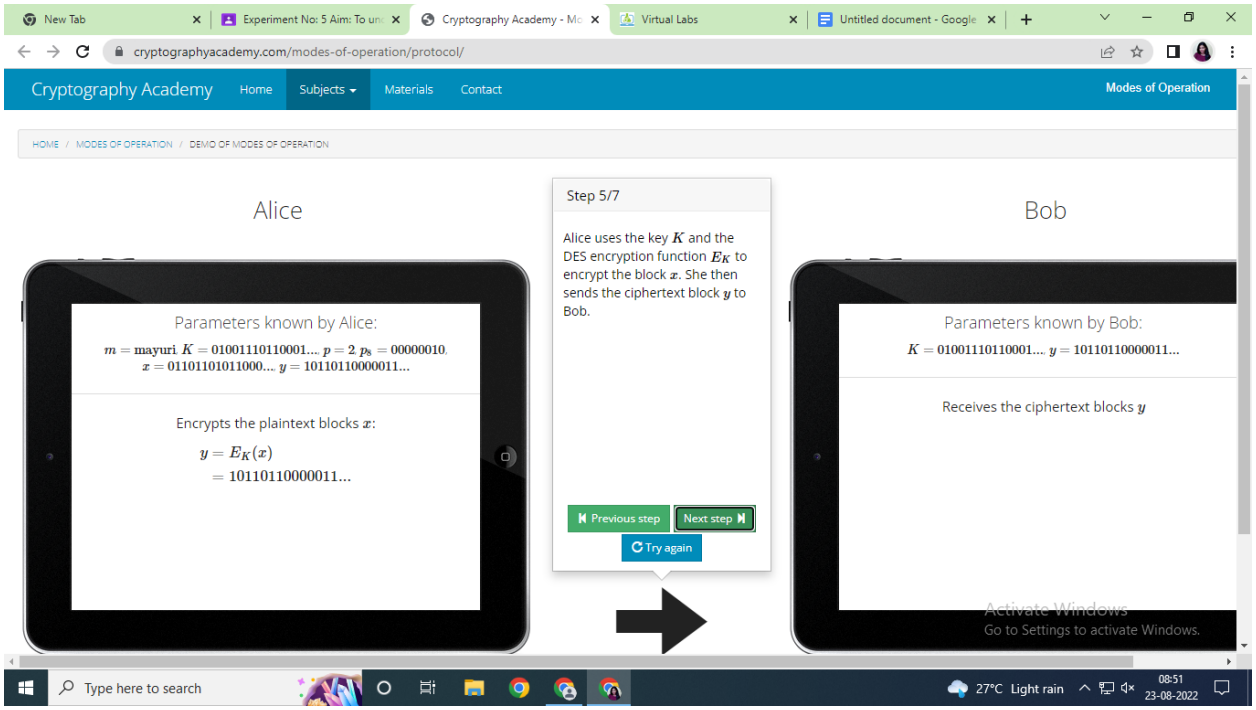
1) DES - ECB

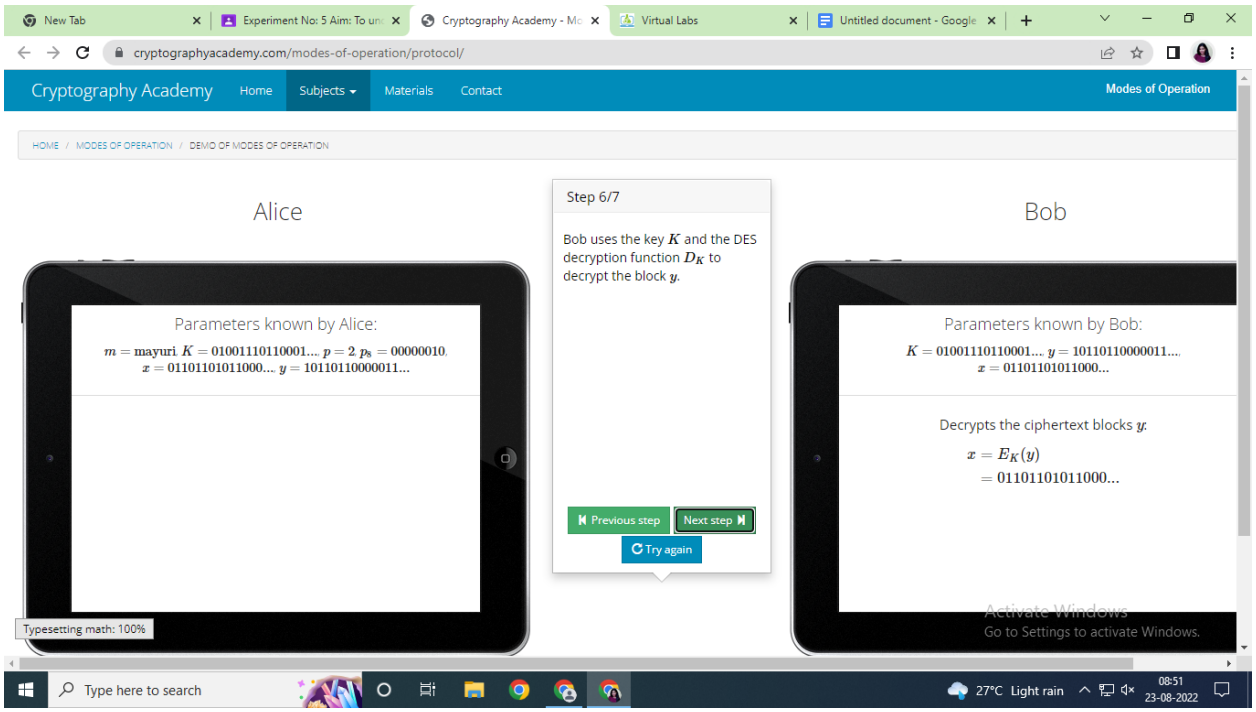


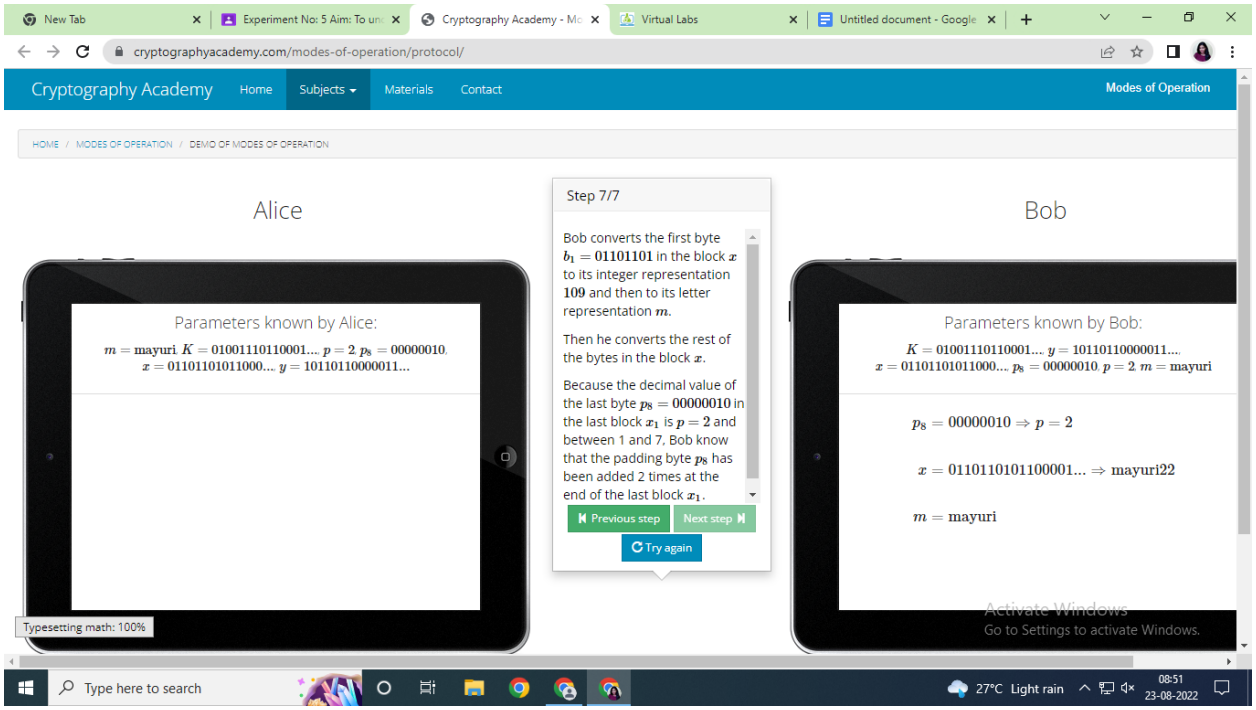



New Tab
Experiment No: 5 Aim: To un
Cryptography Academy - Mc
Virtual Labs
Untitled document - Google
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01001110110001...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01001110110001...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:51
23-08-2022

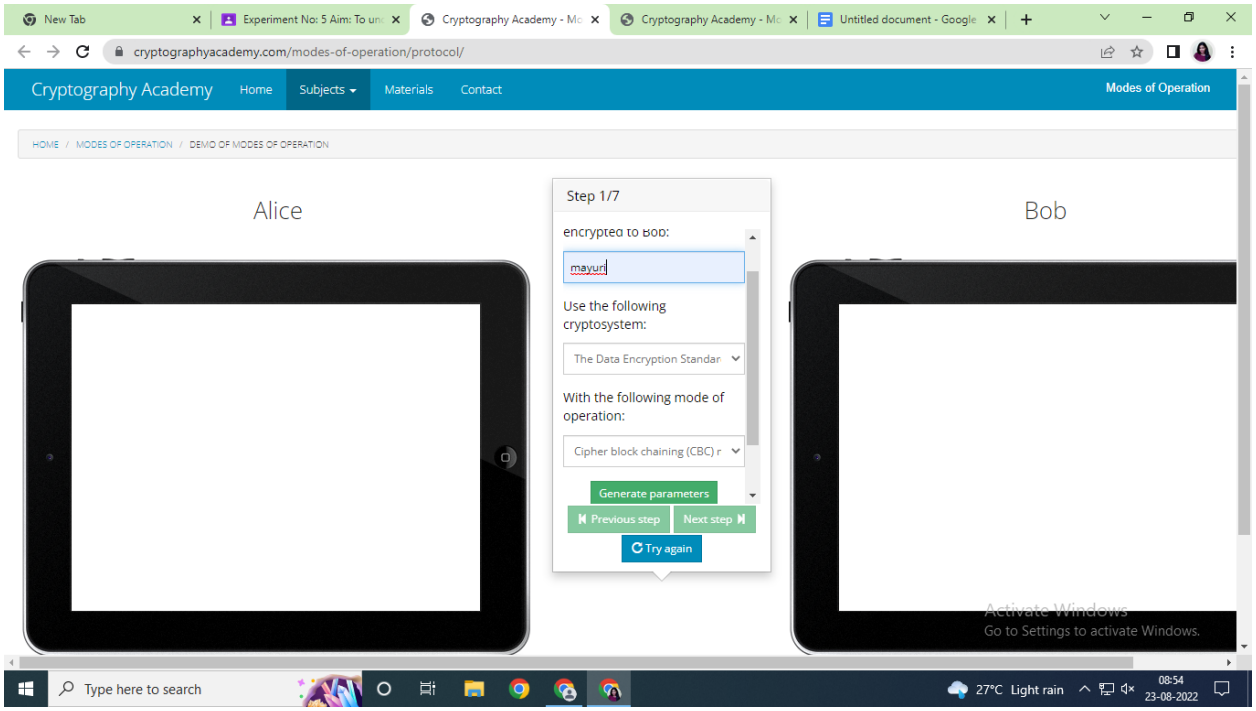

New Tab
Experiment No: 5 Aim: To un
Cryptography Academy - Mc
Virtual Labs
Untitled document - Google
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01001110110001...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$
$p = 6 \; mod \; 8 = 2 \Rightarrow p_8 = 00000010$
$x = \text{mayuri22} \Rightarrow 0110110101100001...$
Step 4/7
DES encrypts blocks of 8 bytes (1 byte is 8 bits so 8 bytes is 64 bits) which corresponds to 8 ASCII characters, because each ASCII character is 1 byte.
The message m contains 6 characters (including whitespace) so we need $p = 6 \; mod \; 8 = 2$ bytes to fill up the last block x_1 such that it's 8 bytes (64 bits). This operation is called padding and it's therefore denoted p.
In binary $p = 2$ is represented
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01001110110001...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:51
23-08-2022

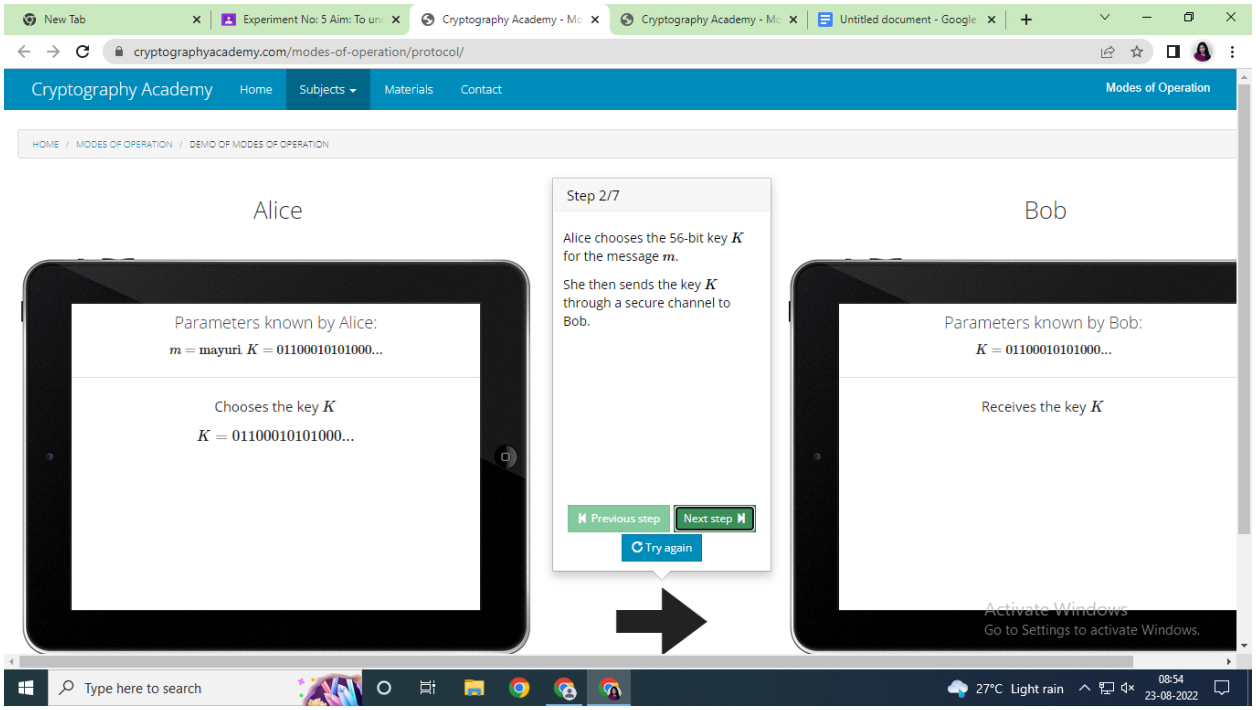

New Tab
Experiment No: 5 Aim: To un
Cryptography Academy - Mc
Virtual Labs
Untitled document - Google
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01001110110001...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$, $y = 10110110000011...$
Encrypts the plaintext blocks x:
$y = E_K(x)$
$= 10110110000011...$
Step 5/7
Alice uses the key K and the DES encryption function E_K to encrypt the block x. She then sends the ciphertext block y to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01001110110001...$, $y = 10110110000011...$
Receives the ciphertext blocks y
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:51
23-08-2022

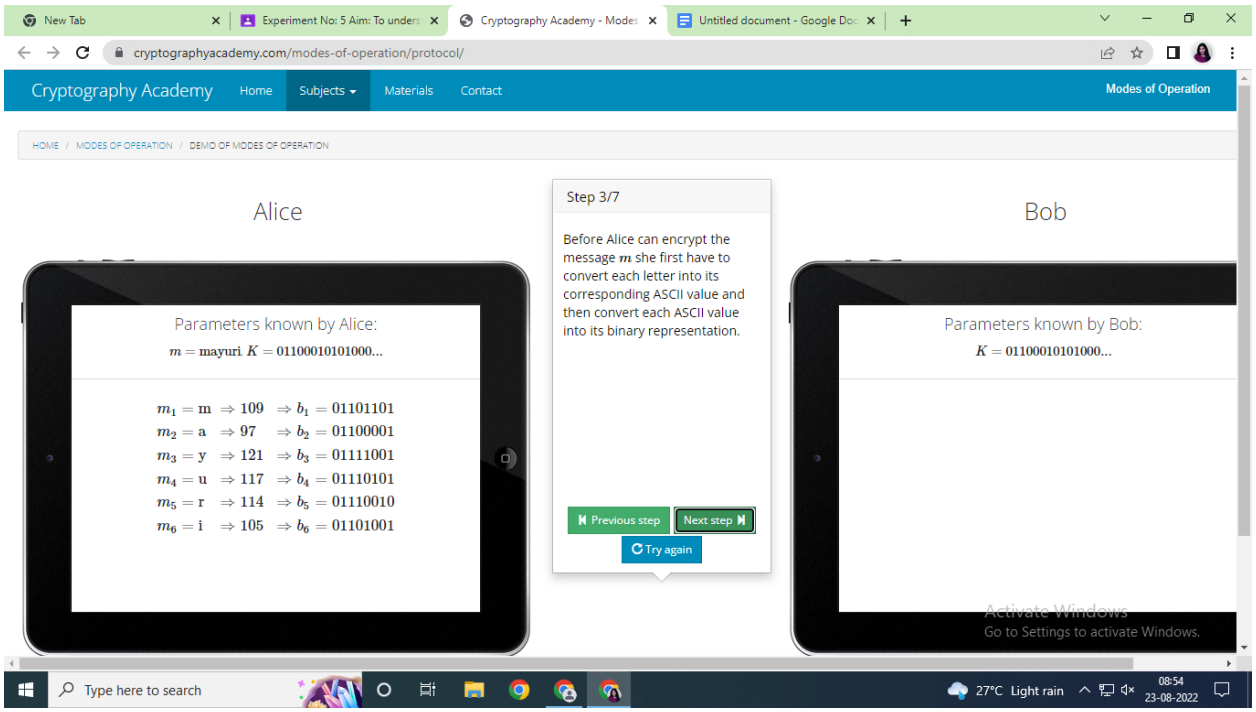

New Tab
Experiment No: 5 Aim: To un
Cryptography Academy - Mc
Virtual Labs
Untitled document - Google
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01001110110001...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$, $y = 10110110000011...$
Step 6/7
Bob uses the key K and the DES decryption function D_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01001110110001...$, $y = 10110110000011...$,
$x = 01101101011000...$
Decrypts the ciphertext blocks y:
$x = E_K(y)$
$= 01101101011000...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:51
23-08-2022

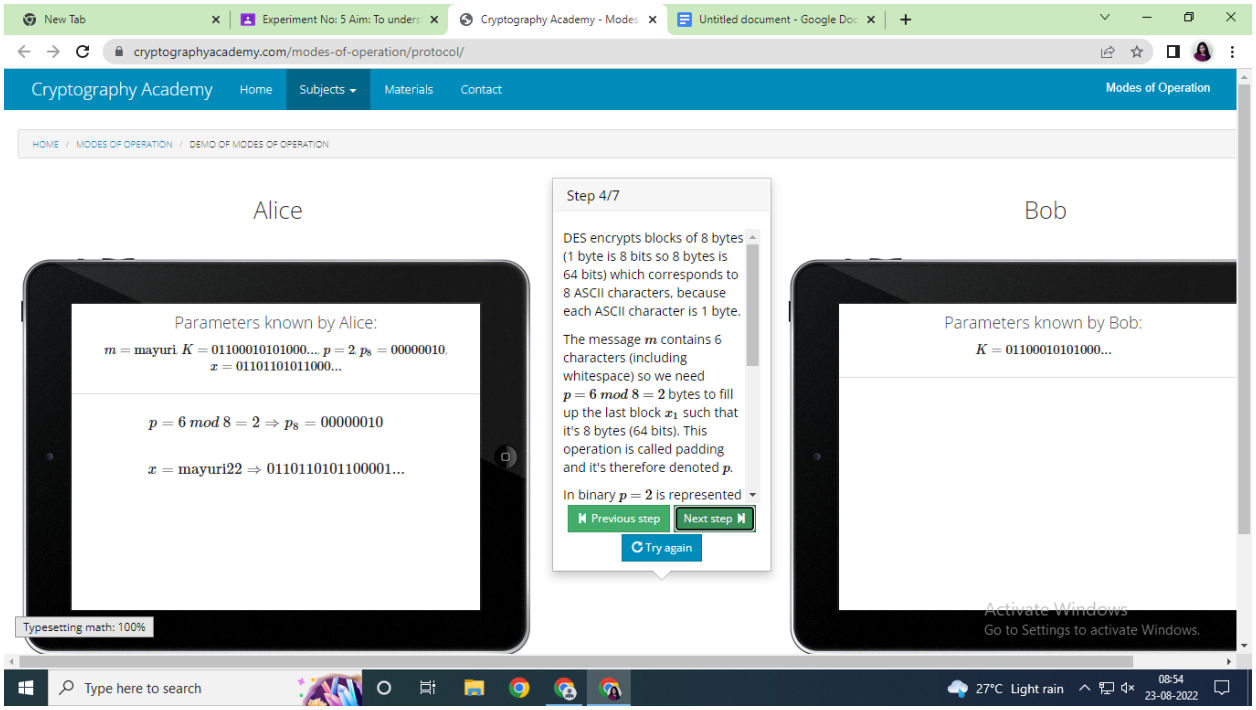

Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 7/7
Bob converts the first byte $b_1 = 01101101$ in the block x to its integer representation 109 and then to its letter representation m.
Then he converts the rest of the bytes in the block x.
Because the decimal value of the last byte $p_8 = 00000010$ in the last block x_1 is $p = 2$ and between 1 and 7, Bob know that the padding byte p_8 has been added 2 times at the end of the last block x_1.
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01001110110001...$, $p = 2$, $p_8 = 00000010$, $x = 01101101011000...$, $y = 10110110000011...$
Parameters known by Bob:
$K = 01001110110001...$, $y = 10110110000011...$, $x = 01101101011000...$, $p_8 = 00000010$, $p = 2$, $m = \text{mayuri}$
$p_8 = 00000010 \Rightarrow p = 2$
$x = 0110110101100001... \Rightarrow \text{mayuri22}$
$m = \text{mayuri}$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:51
23-08-2022

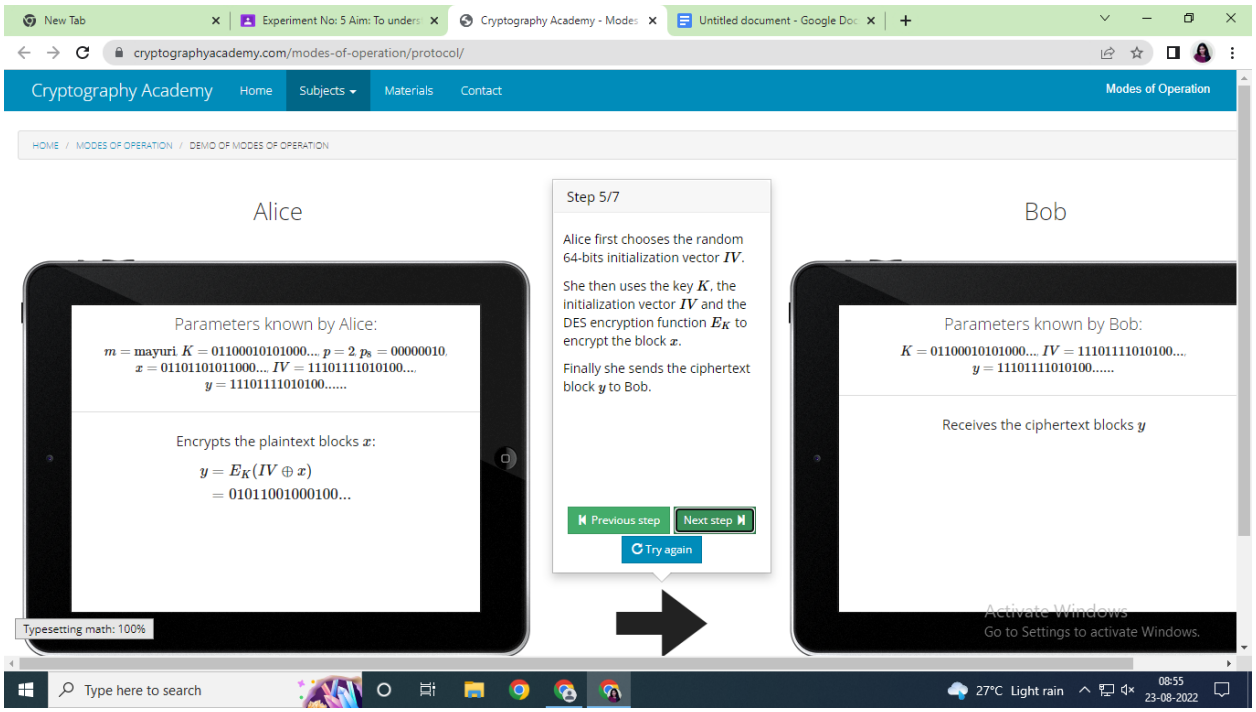
2) DES - CBC

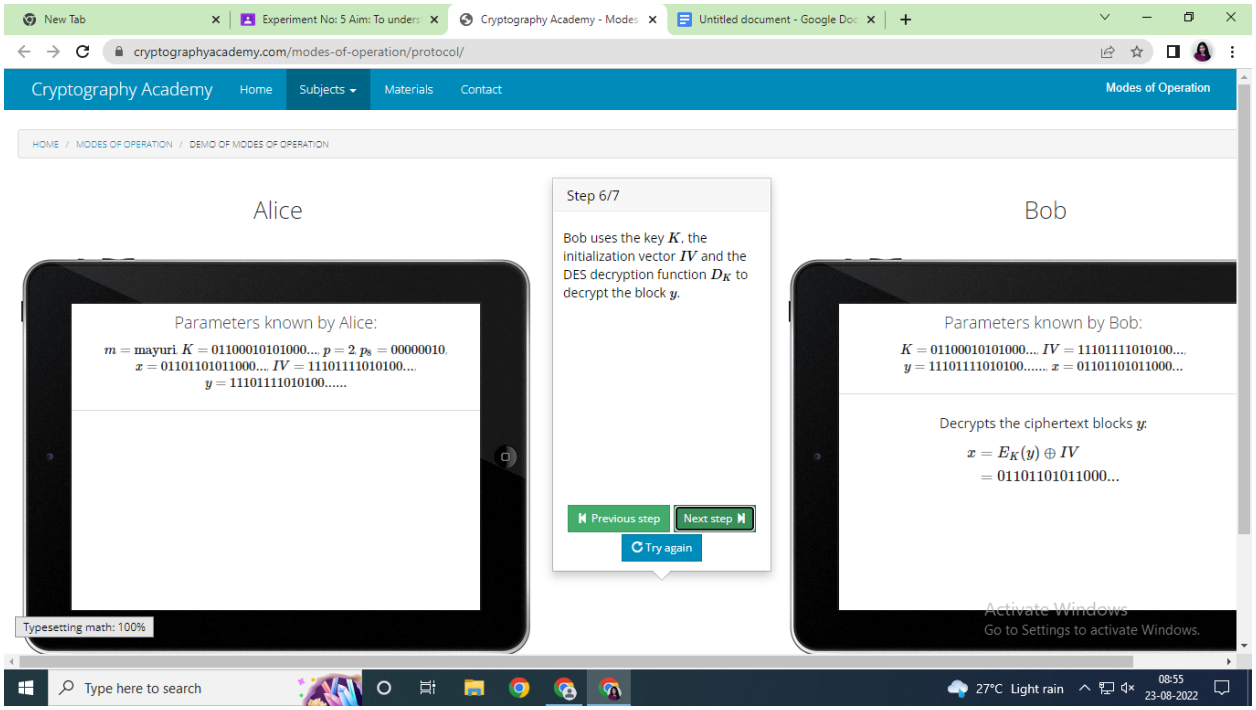

Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 1/7
encrypted to Bob:
mayuri
Use the following cryptosystem:
The Data Encryption Standar
With the following mode of operation:
Cipher block chaining (CBC) r
Generate parameters
Previous step
Next step
Try again
Bob
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:54
23-08-2022

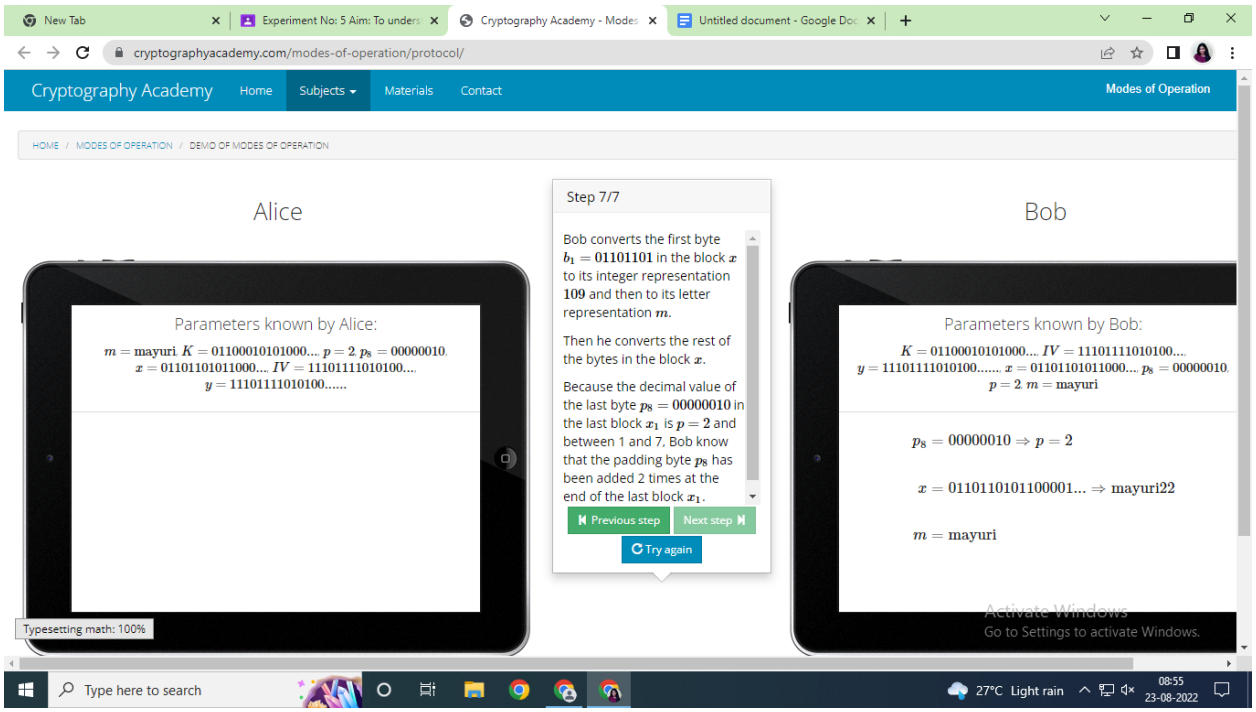

New Tab
Experiment No: 5 Aim: To un
Cryptography Academy - Mc
Cryptography Academy - Mc
Untitled document - Google
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 2/7
Alice chooses the 56-bit key K for the message m.
She then sends the key K through a secure channel to Bob.
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 01100010101000...$
Chooses the key K
$K = 01100010101000...$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 01100010101000...$
Receives the key K
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:54
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 01100010101000...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 01100010101000...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:54
23-08-2022

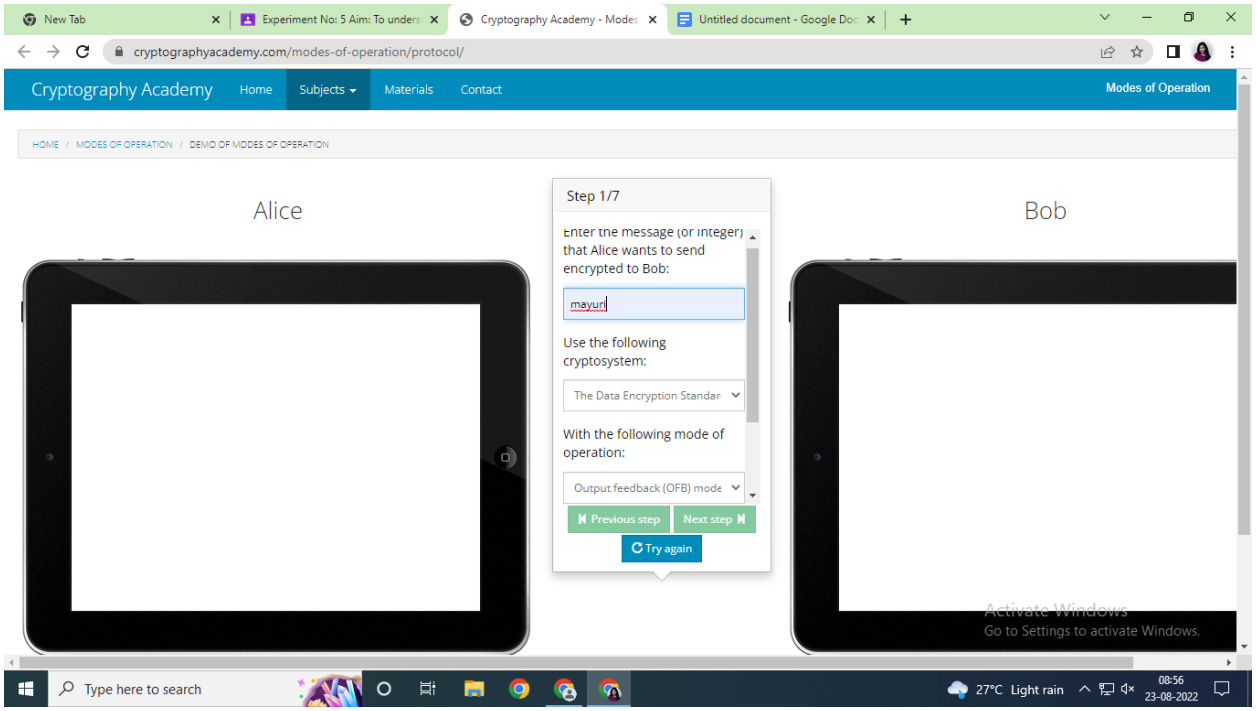

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 4/7
DES encrypts blocks of 8 bytes (1 byte is 8 bits so 8 bytes is 64 bits) which corresponds to 8 ASCII characters, because each ASCII character is 1 byte.
The message m contains 6 characters (including whitespace) so we need $p = 6 \ mod \ 8 = 2$ bytes to fill up the last block x_1 such that it's 8 bytes (64 bits). This operation is called padding and it's therefore denoted p.
In binary $p = 2$ is represented
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01100010101000...$, $p = 2$, $p_8 = 00000010$, $x = 01101101011000...$
$p = 6 \ mod \ 8 = 2 \Rightarrow p_8 = 00000010$
$x = \text{mayuri22} \Rightarrow 0110110101100001...$
Parameters known by Bob:
$K = 01100010101000...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:54
23-08-2022

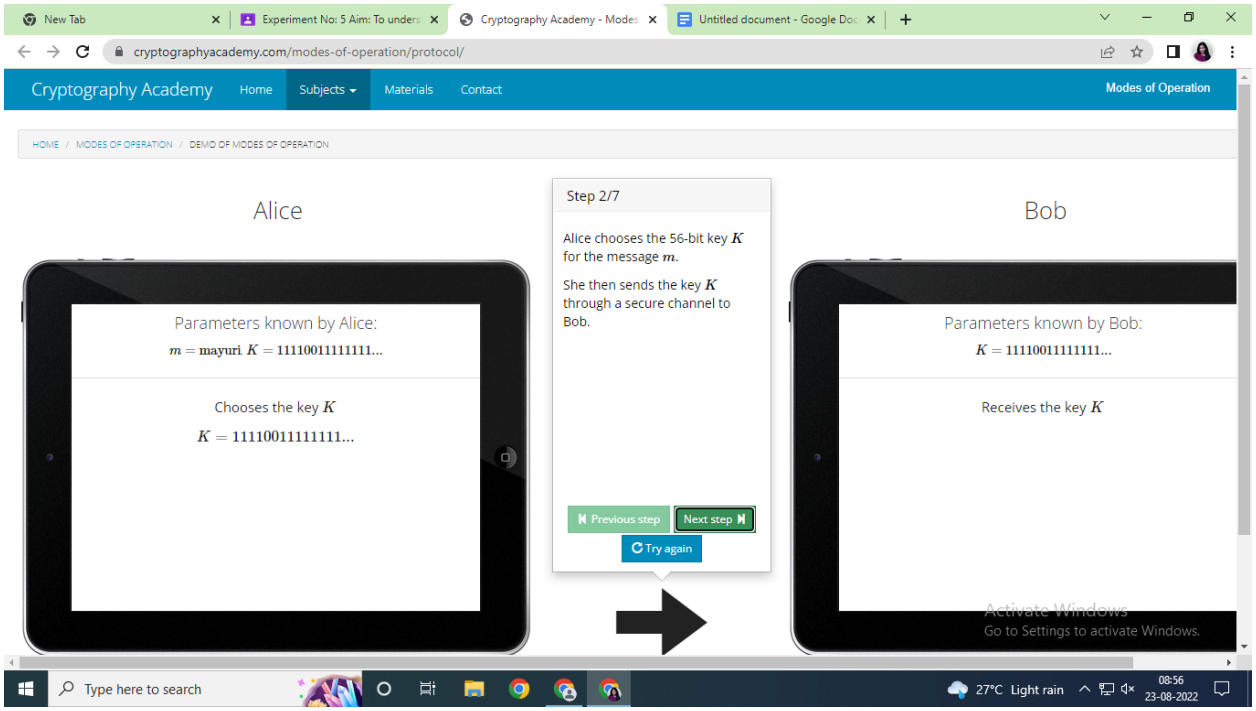

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 5/7
Alice first chooses the random 64-bits initialization vector IV.
She then uses the key K, the initialization vector IV and the DES encryption function E_K to encrypt the block x.
Finally she sends the ciphertext block y to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01100010101000...$, $p = 2$, $p_8 = 00000010$, $x = 01101101011000...$, $IV = 11101111010100...$, $y = 11101111010100.....$
Encrypts the plaintext blocks x:
$y = E_K(IV \oplus x)$
$= 01011001000100...$
Parameters known by Bob:
$K = 01100010101000...$, $IV = 11101111010100...$, $y = 11101111010100.....$
Receives the ciphertext blocks y
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:55
23-08-2022

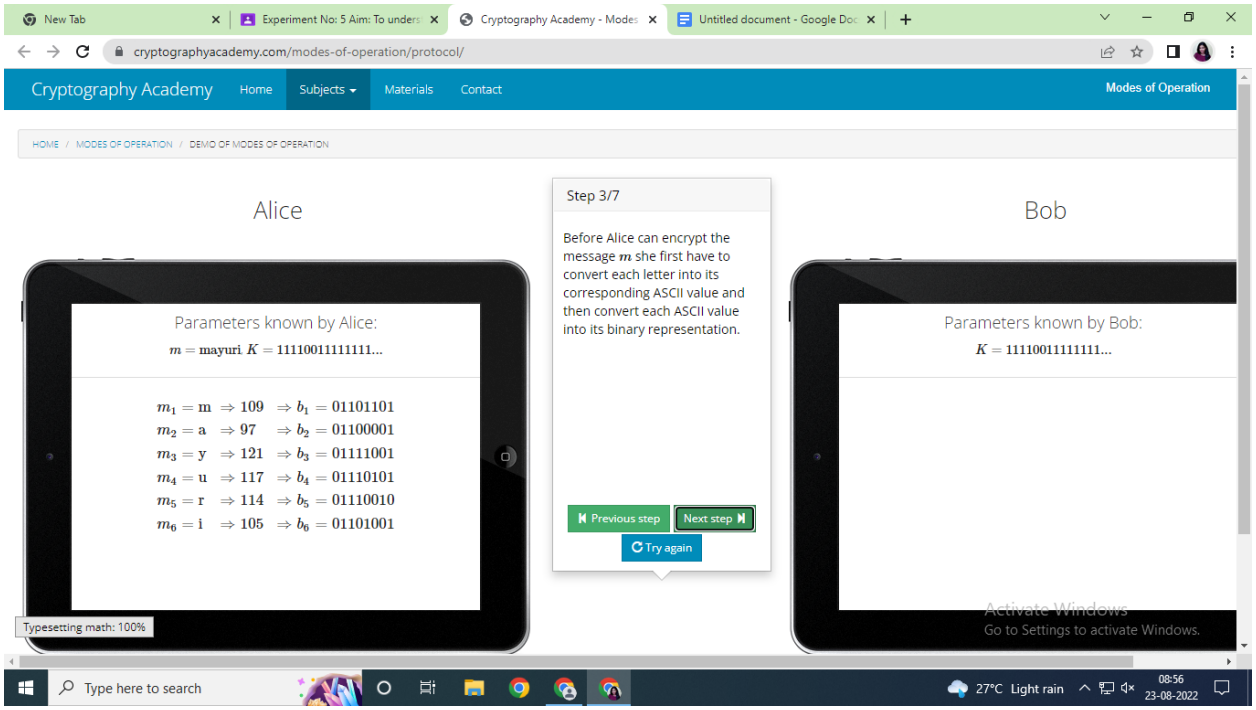

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01100010101000...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$, $IV = 11101111010100...$,
$y = 11101111010100.....$
Typesetting math: 100%
Step 6/7
Bob uses the key K, the initialization vector IV and the DES decryption function D_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01100010101000...$, $IV = 11101111010100...$,
$y = 11101111010100.....$, $x = 01101101011000...$
Decrypts the ciphertext blocks y:
$x = E_K(y) \oplus IV$
$= 01101101011000...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:55
23-08-2022

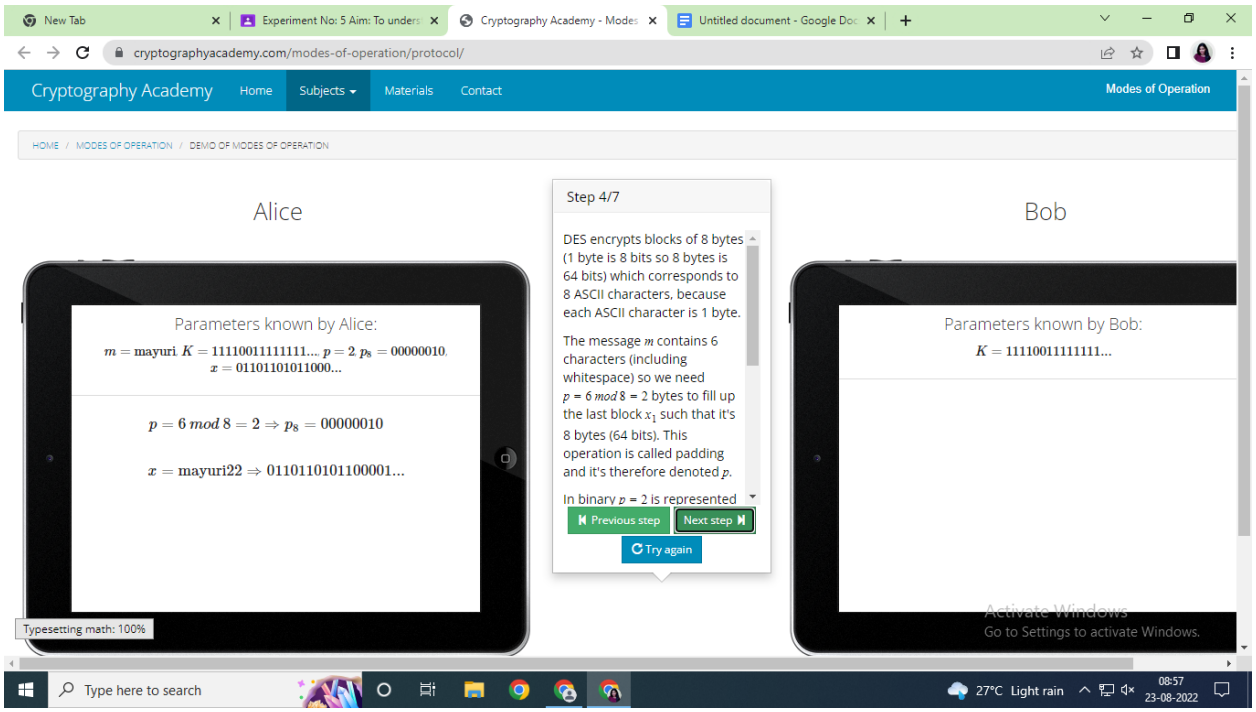

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01100010101000...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$, $IV = 11101111010100...$,
$y = 11101111010100.....$
Typesetting math: 100%
Step 7/7
Bob converts the first byte $b_1 = 01101101$ in the block x to its integer representation 109 and then to its letter representation m.
Then he converts the rest of the bytes in the block x.
Because the decimal value of the last byte $p_8 = 00000010$ in the last block x_1 is $p = 2$ and between 1 and 7, Bob know that the padding byte p_8 has been added 2 times at the end of the last block x_1.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01100010101000...$, $IV = 11101111010100...$,
$y = 11101111010100.....$, $x = 01101101011000...$, $p_8 = 00000010$,
$p = 2$, $m = \text{mayuri}$
$p_8 = 00000010 \Rightarrow p = 2$
$x = 0110110101100001... \Rightarrow \text{mayuri22}$
$m = \text{mayuri}$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:55
23-08-2022

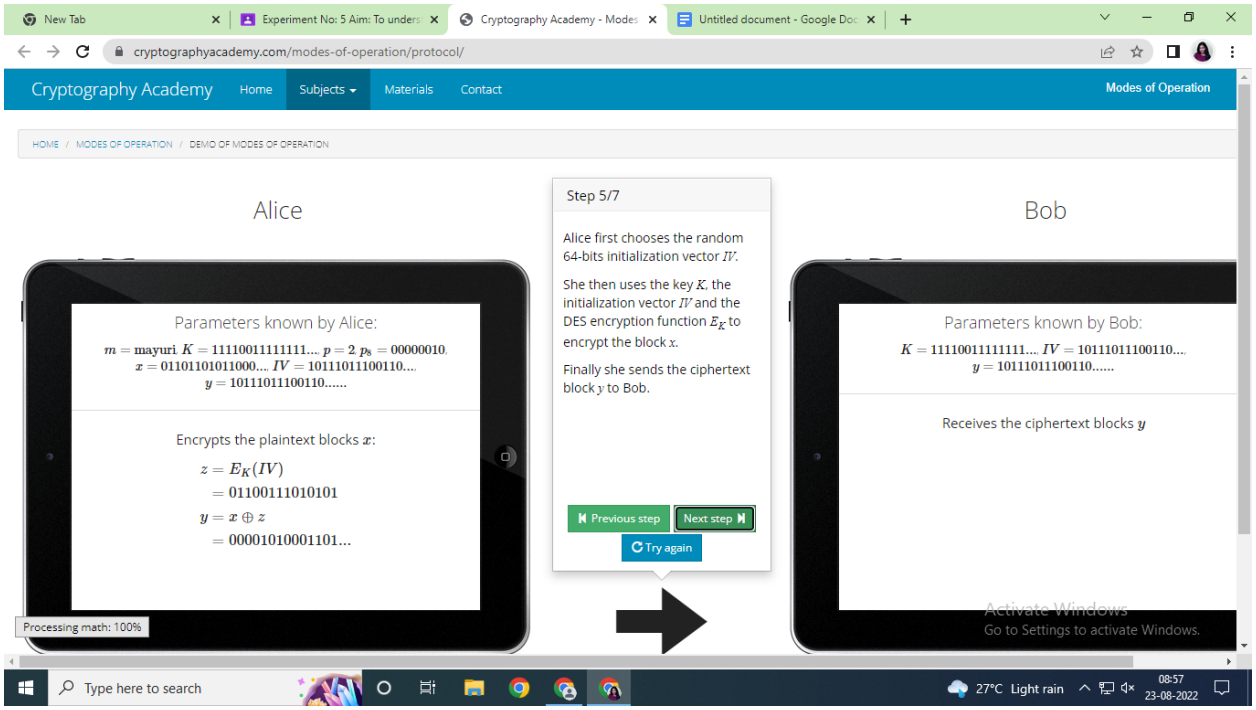
3) DES - OFB

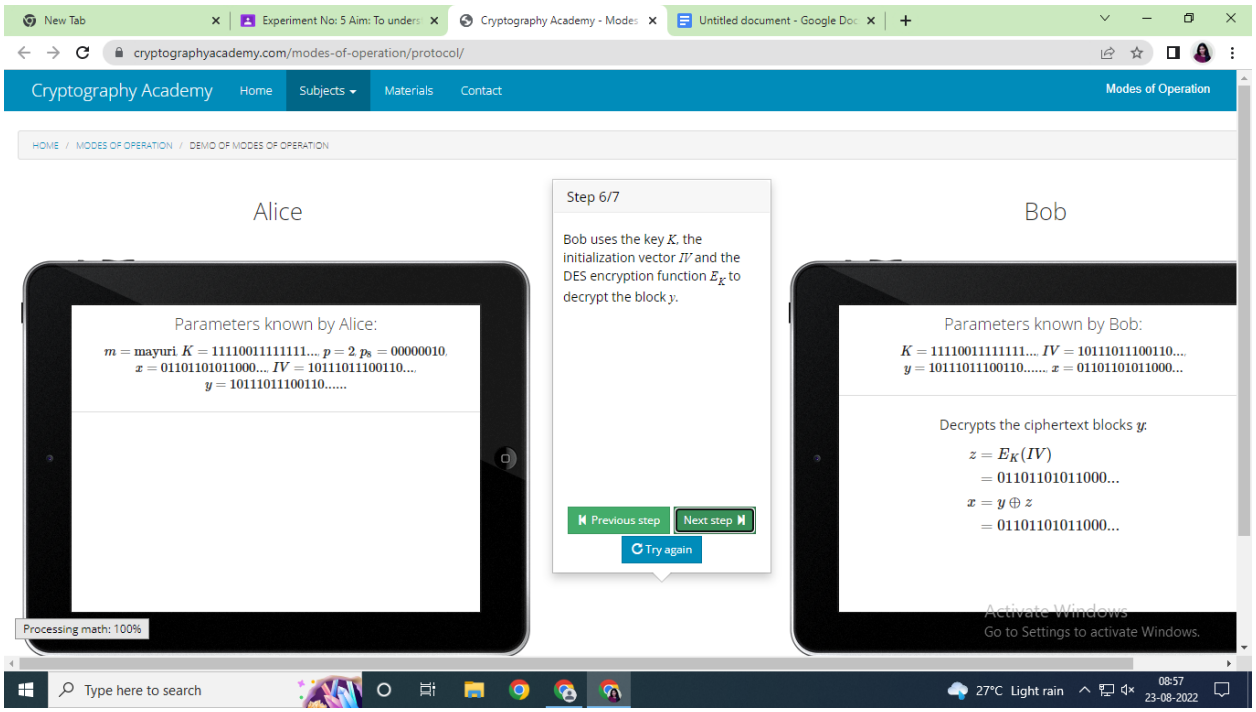

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 1/7
Enter the message (or integer) that Alice wants to send encrypted to Bob:
mayuri
Use the following cryptosystem:
The Data Encryption Standar
With the following mode of operation:
Output feedback (OFB) mode
Previous step
Next step
Try again
Bob
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:56
23-08-2022

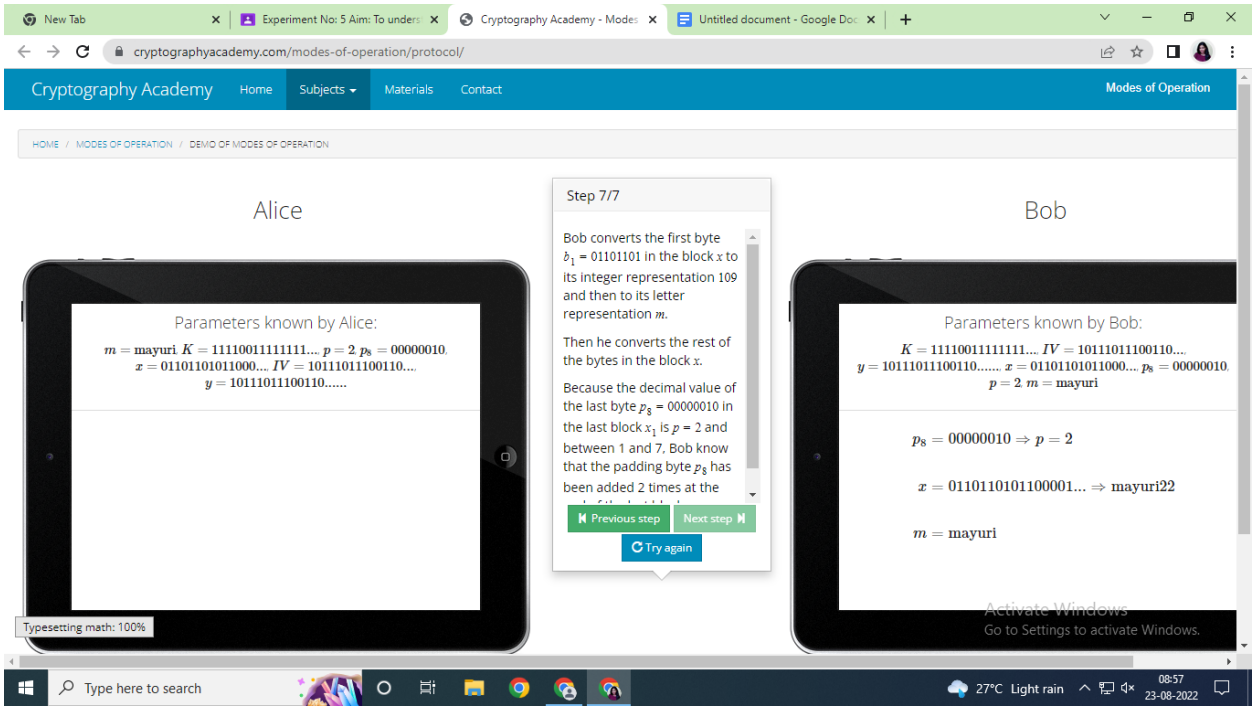

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 11110011111111...$
Chooses the key K
$K = 11110011111111...$
Step 2/7
Alice chooses the 56-bit key K for the message m.
She then sends the key K through a secure channel to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11110011111111...$
Receives the key K
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:56
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 11110011111111...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 11110011111111...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:56
23-08-2022

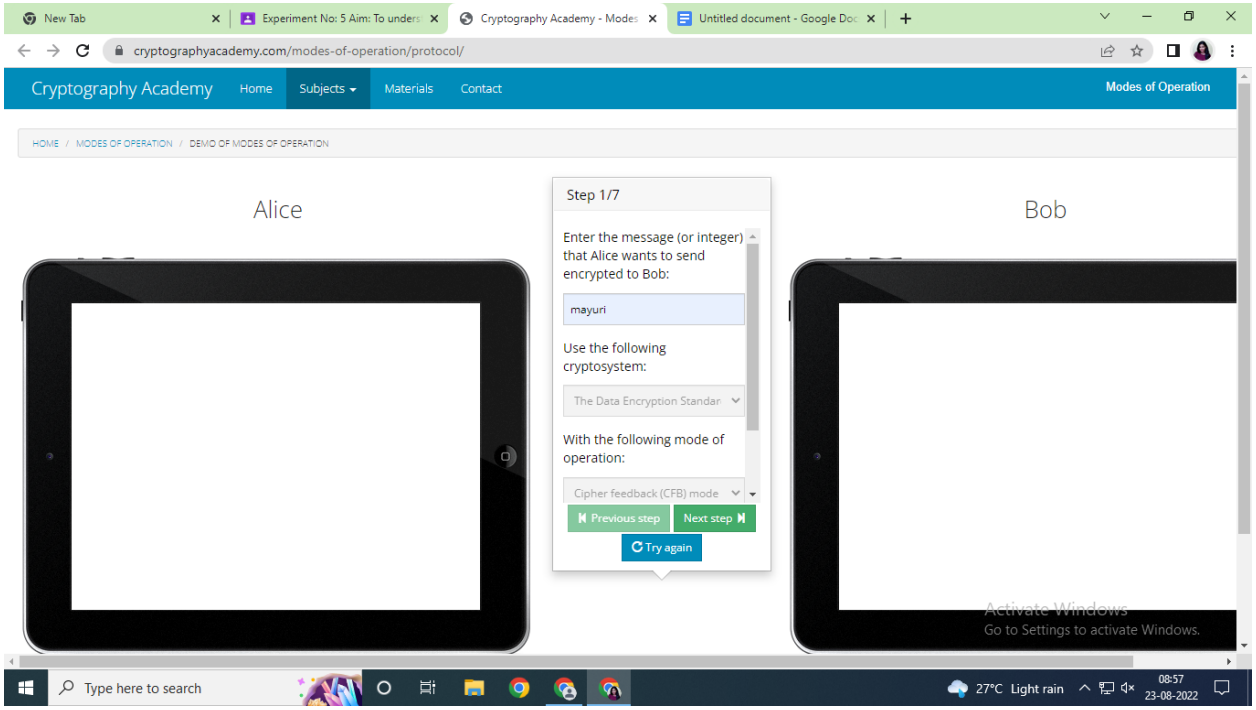

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 4/7
DES encrypts blocks of 8 bytes (1 byte is 8 bits so 8 bytes is 64 bits) which corresponds to 8 ASCII characters, because each ASCII character is 1 byte.
The message m contains 6 characters (including whitespace) so we need $p = 6 \ mod \ 8 = 2$ bytes to fill up the last block x_1 such that it's 8 bytes (64 bits). This operation is called padding and it's therefore denoted p.
In binary $p = 2$ is represented
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 11110011111111...$ $p = 2$ $p_8 = 00000010$
$x = 01101101011000...$
$p = 6 \ mod \ 8 = 2 \Rightarrow p_8 = 00000010$
$x = \text{mayuri22} \Rightarrow 01101101011000001...$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 11110011111111...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:57
23-08-2022

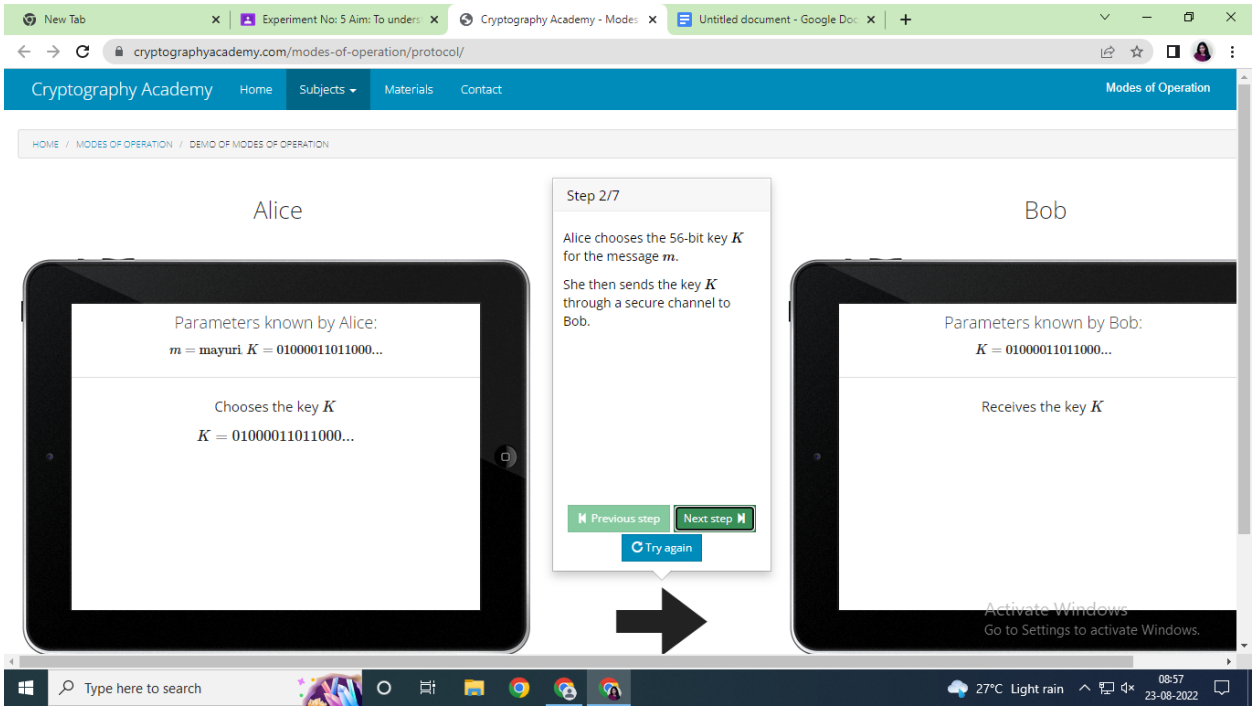

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 11110011111111....$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000....$, $IV = 10111011100110....$,
$y = 10111011100110.....$
Encrypts the plaintext blocks x:
$z = E_K(IV)$
$= 01100111010101$
$y = x \oplus z$
$= 00001010001101...$
Processing math: 100%
Step 5/7
Alice first chooses the random 64-bits initialization vector IV.
She then uses the key K, the initialization vector IV and the DES encryption function E_K to encrypt the block x.
Finally she sends the ciphertext block y to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11110011111111....$, $IV = 10111011100110....$,
$y = 10111011100110.....$
Receives the ciphertext blocks y
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:57
23-08-2022

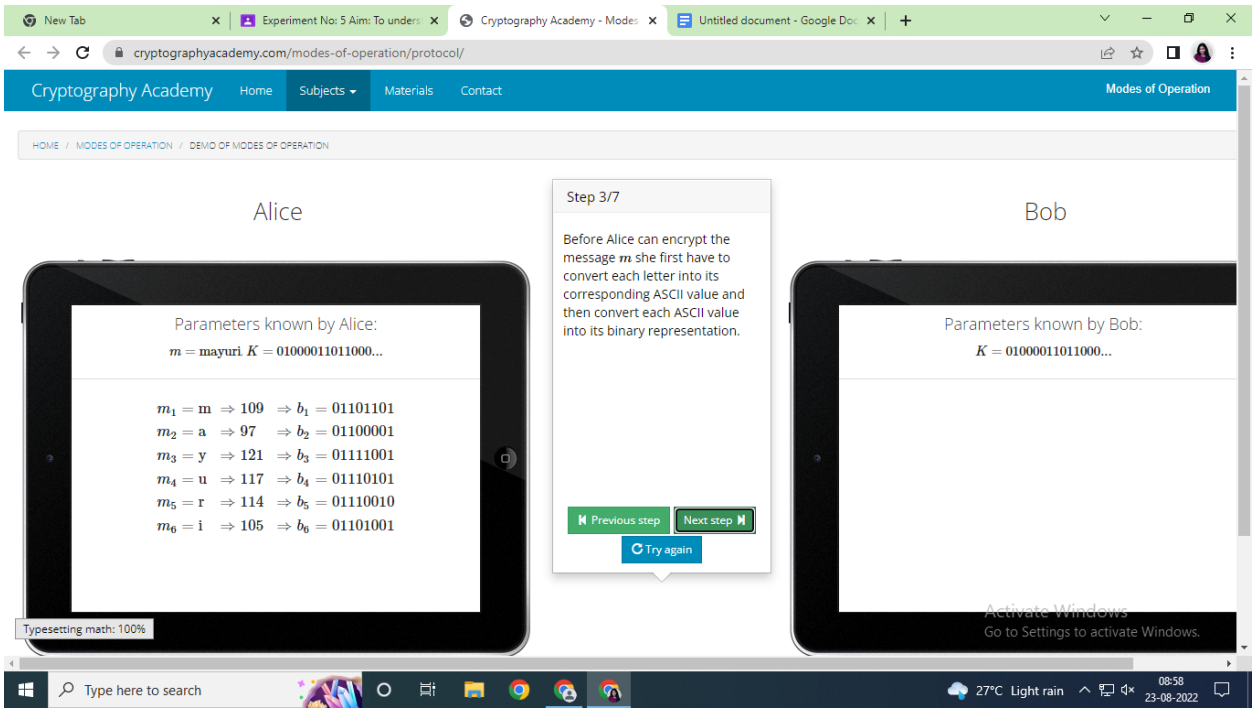

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 11110011111111....$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000....$, $IV = 10111011100110....$,
$y = 10111011100110.....$
Processing math: 100%
Step 6/7
Bob uses the key K, the initialization vector IV and the DES encryption function E_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11110011111111....$, $IV = 10111011100110....$,
$y = 10111011100110.....$, $x = 01101101011000...$
Decrypts the ciphertext blocks y:
$z = E_K(IV)$
$= 01101101011000...$
$x = y \oplus z$
$= 01101101011000...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:57
23-08-2022

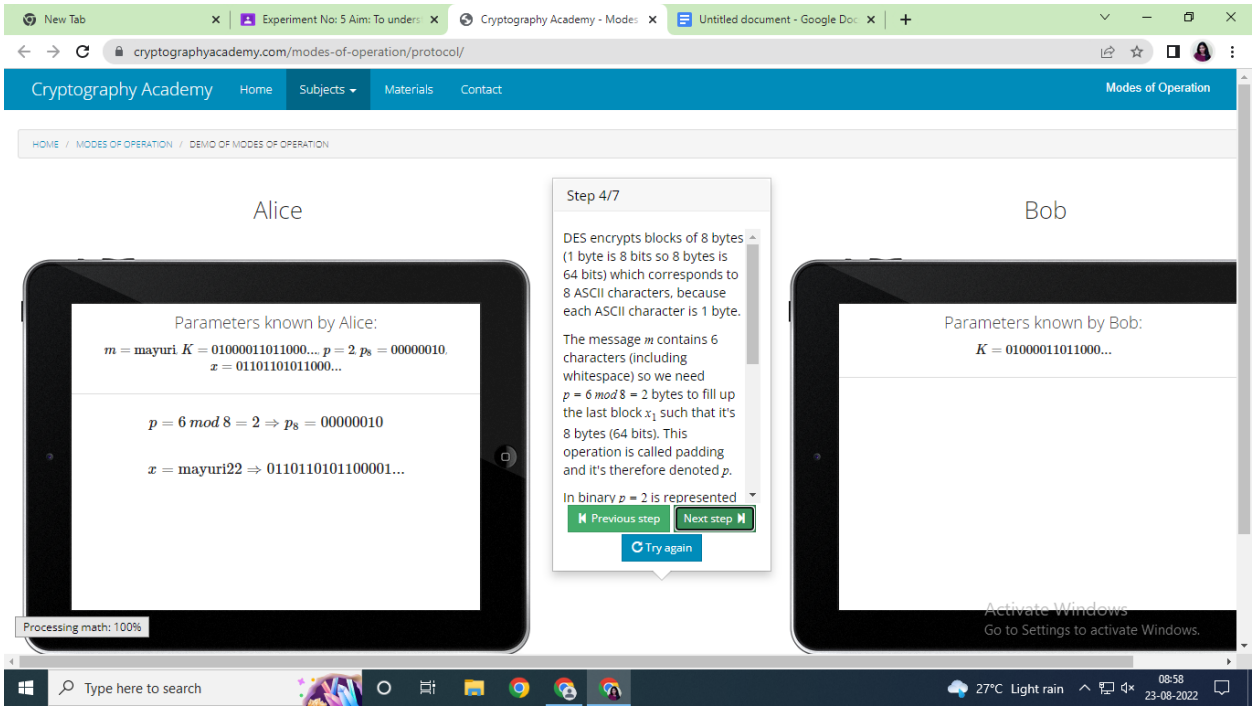

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 11110011111111....$ $p = 2$, $p_8 = 00000010$,
$x = 01101101011000....$ $IV = 10111011100110....$,
$y = 10111011100110.....$
Step 7/7
Bob converts the first byte b_1 = 01101101 in the block x to its integer representation 109 and then to its letter representation m.
Then he converts the rest of the bytes in the block x.
Because the decimal value of the last byte p_8 = 00000010 in the last block x_1 is p = 2 and between 1 and 7, Bob know that the padding byte p_8 has been added 2 times at the
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11110011111111....$ $IV = 10111011100110....$
$y = 10111011100110.....$, $x = 01101101011000....$ $p_8 = 00000010$,
$p = 2$, $m = \text{mayuri}$
$p_8 = 00000010 \Rightarrow p = 2$
$x = 0110110101100001... \Rightarrow \text{mayuri22}$
$m = \text{mayuri}$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:57
23-08-2022

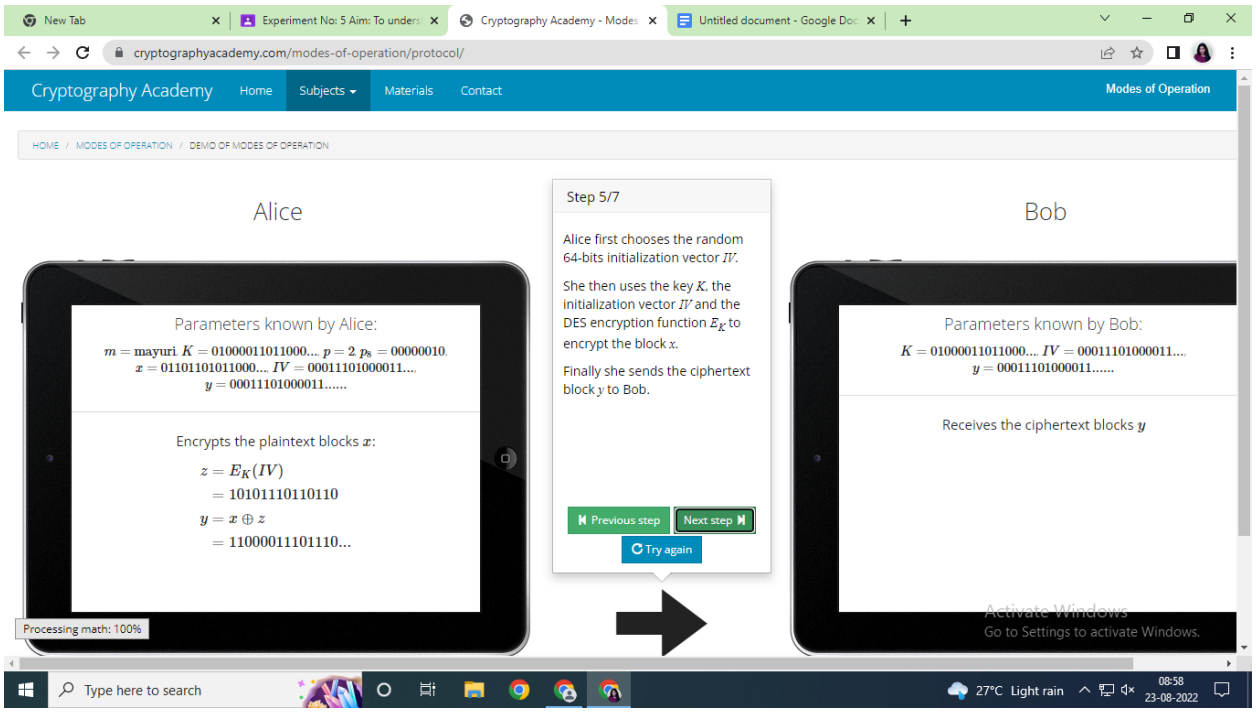
4) DES - CFB

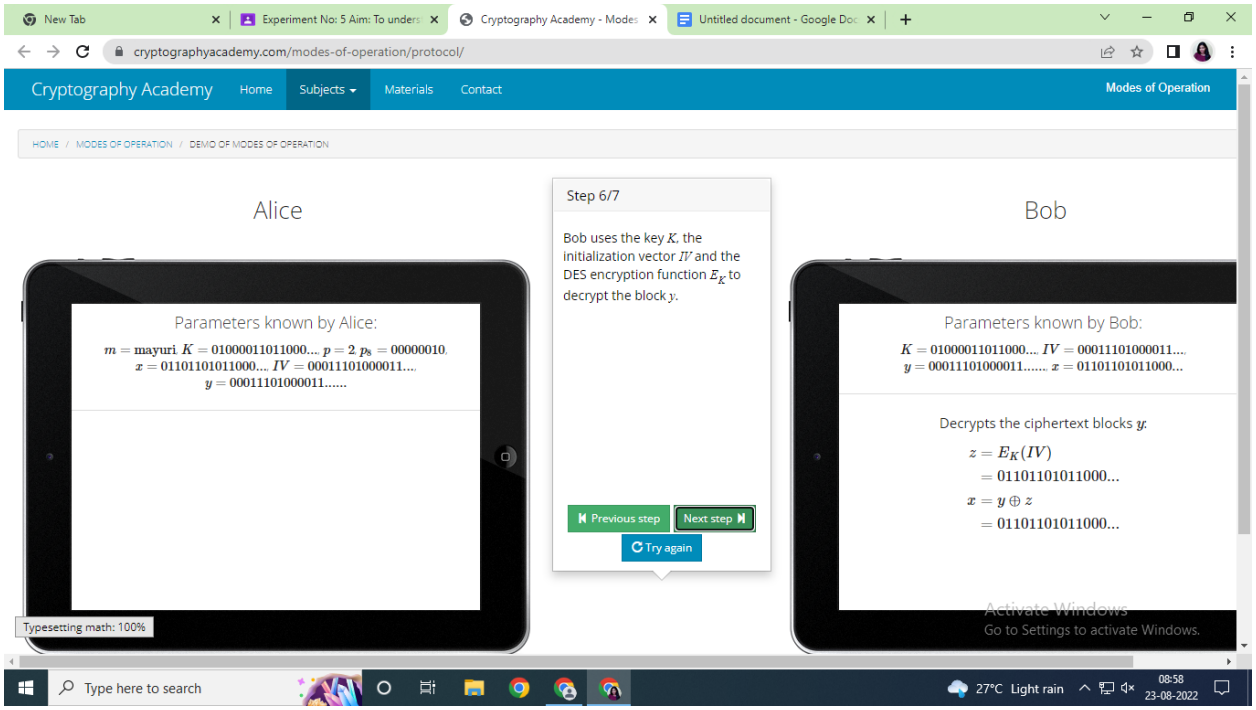

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 1/7
Enter the message (or integer) that Alice wants to send encrypted to Bob:
mayuri
Use the following cryptosystem:
The Data Encryption Standar
With the following mode of operation:
Cipher feedback (CFB) mode
Previous step
Next step
Try again
Bob
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:57
23-08-2022

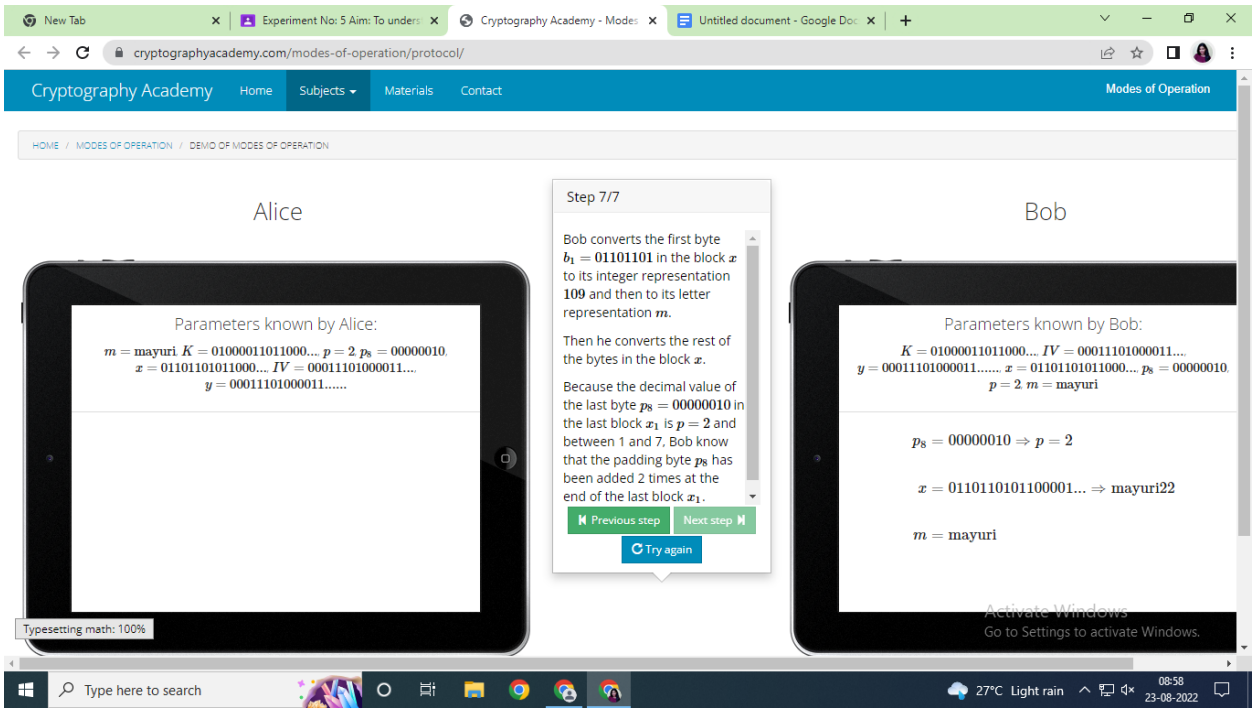

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 01000011011000...$
Chooses the key K
$K = 01000011011000...$
Step 2/7
Alice chooses the 56-bit key K for the message m.
She then sends the key K through a secure channel to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01000011011000...$
Receives the key K
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:57
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 01000011011000...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Typesetting math: 100%
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01000011011000...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:58
23-08-2022

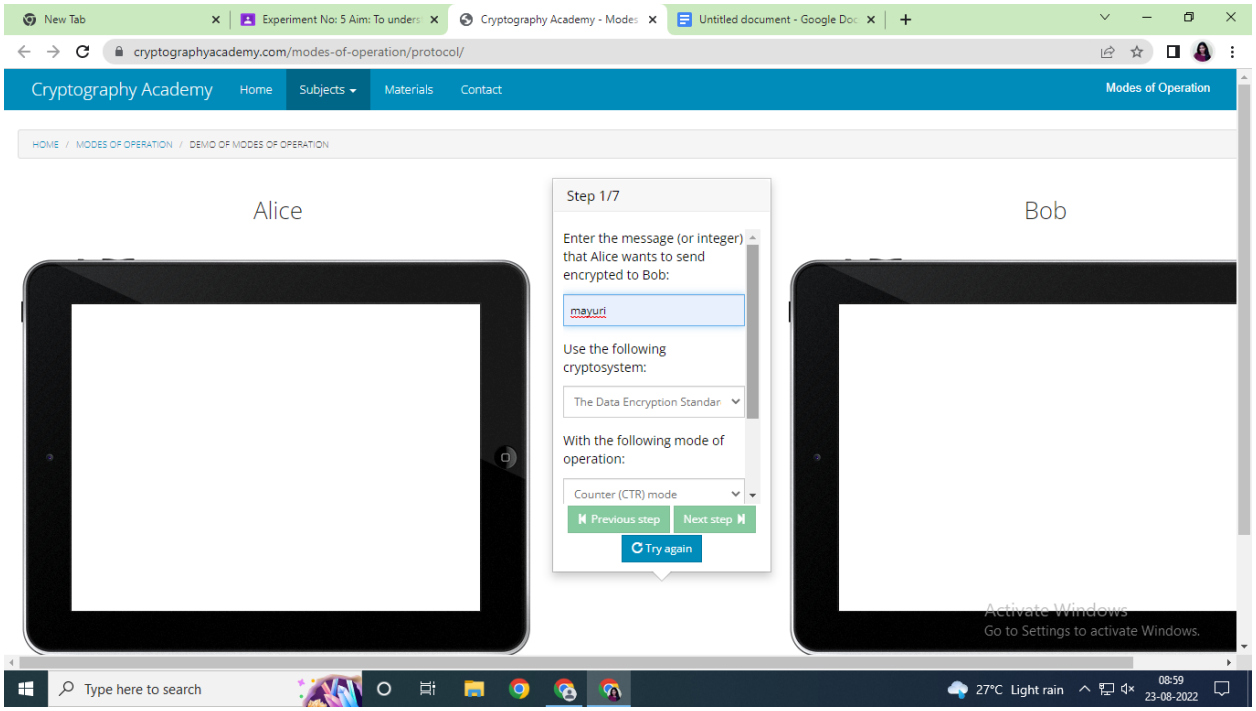

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 4/7
DES encrypts blocks of 8 bytes (1 byte is 8 bits so 8 bytes is 64 bits) which corresponds to 8 ASCII characters, because each ASCII character is 1 byte.
The message m contains 6 characters (including whitespace) so we need $p = 6 \ mod \ 8 = 2$ bytes to fill up the last block x_1 such that it's 8 bytes (64 bits). This operation is called padding and it's therefore denoted p.
In binary $p = 2$ is represented
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01000011011000...$, $p = 2$, $p_8 = 00000010$, $x = 01101101011000...$
$p = 6 \ mod \ 8 = 2 \Rightarrow p_8 = 00000010$
$x = \text{mayuri22} \Rightarrow 0110110101100001...$
Parameters known by Bob:
$K = 01000011011000...$
Processing math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:58
23-08-2022

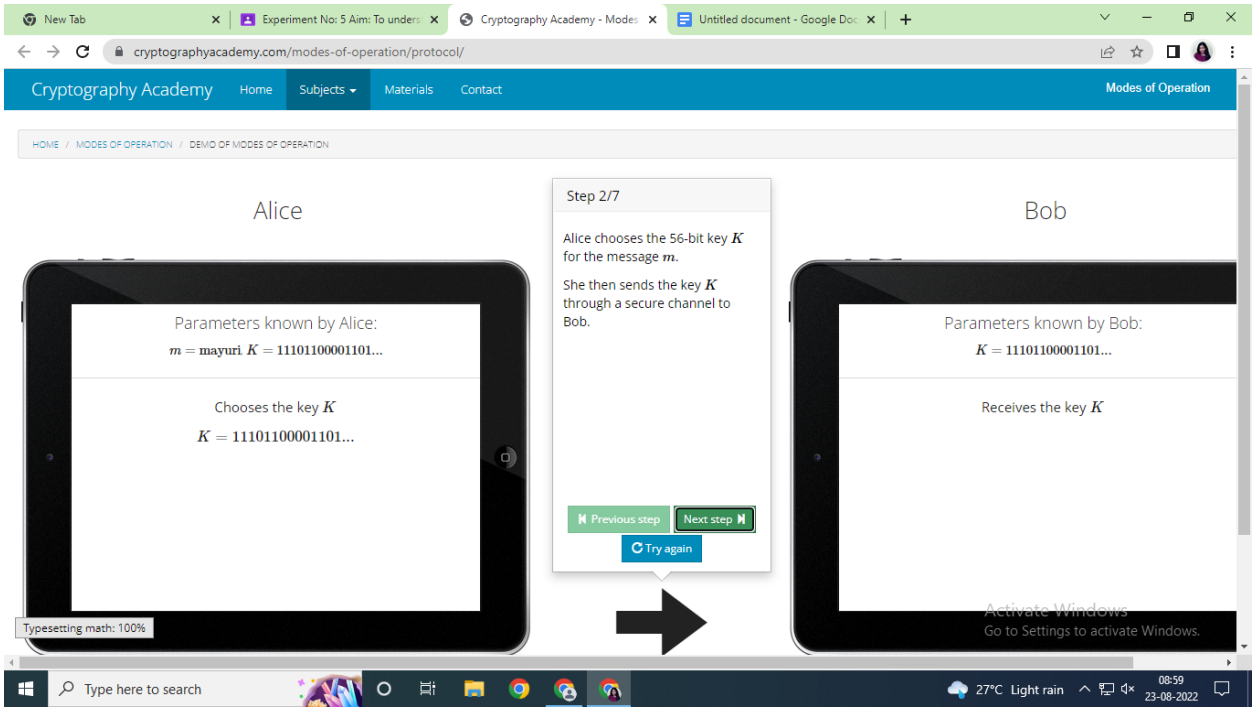

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 5/7
Alice first chooses the random 64-bits initialization vector IV.
She then uses the key K, the initialization vector IV and the DES encryption function E_K to encrypt the block x.
Finally she sends the ciphertext block y to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01000011011000...$, $p = 2$, $p_8 = 00000010$, $x = 01101101011000...$, $IV = 00011101000011...$, $y = 00011101000011.....$
Encrypts the plaintext blocks x:
$z = E_K(IV)$
$= 10101110110110$
$y = x \oplus z$
$= 11000011101110...$
Parameters known by Bob:
$K = 01000011011000...$, $IV = 00011101000011...$, $y = 00011101000011.....$
Receives the ciphertext blocks y
Processing math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:58
23-08-2022

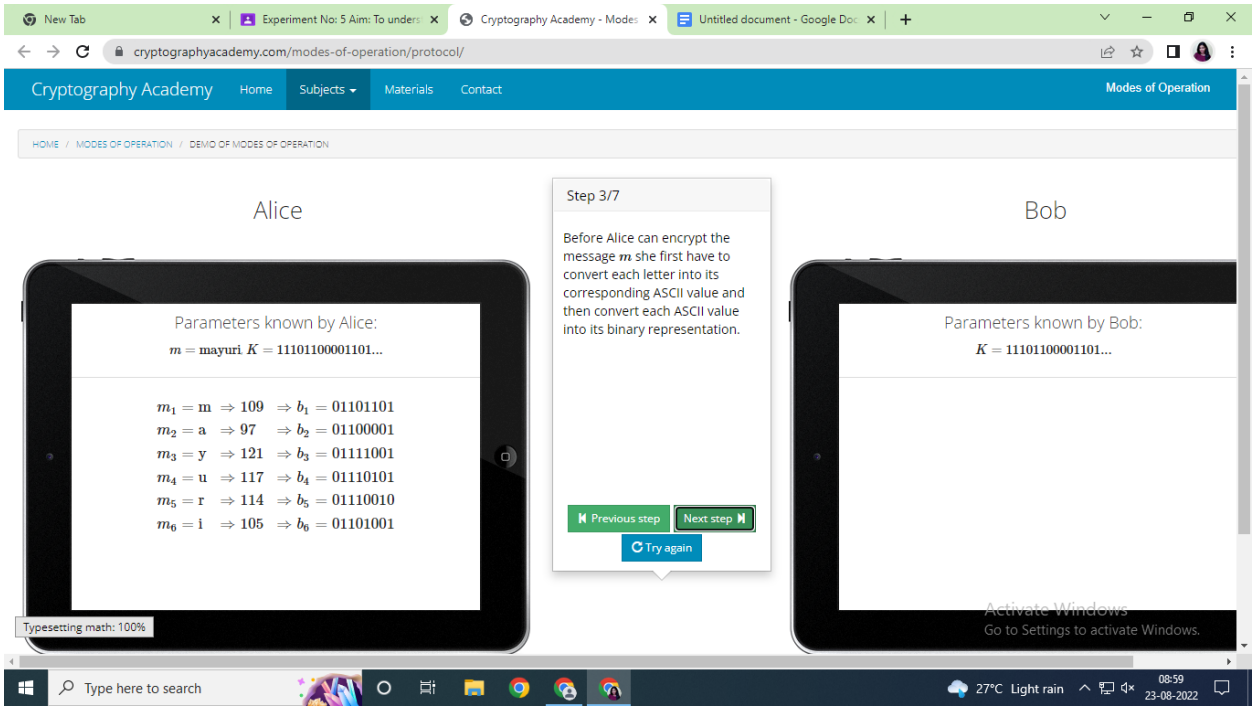

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01000011011000...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$, $IV = 00011101000011...$,
$y = 00011101000011.....$
Typesetting math: 100%
Step 6/7
Bob uses the key K, the initialization vector IV and the DES encryption function E_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01000011011000...$, $IV = 00011101000011...$,
$y = 00011101000011.....$, $x = 01101101011000...$
Decrypts the ciphertext blocks y:
$z = E_K(IV)$
$= 01101101011000...$
$x = y \oplus z$
$= 01101101011000...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:58
23-08-2022

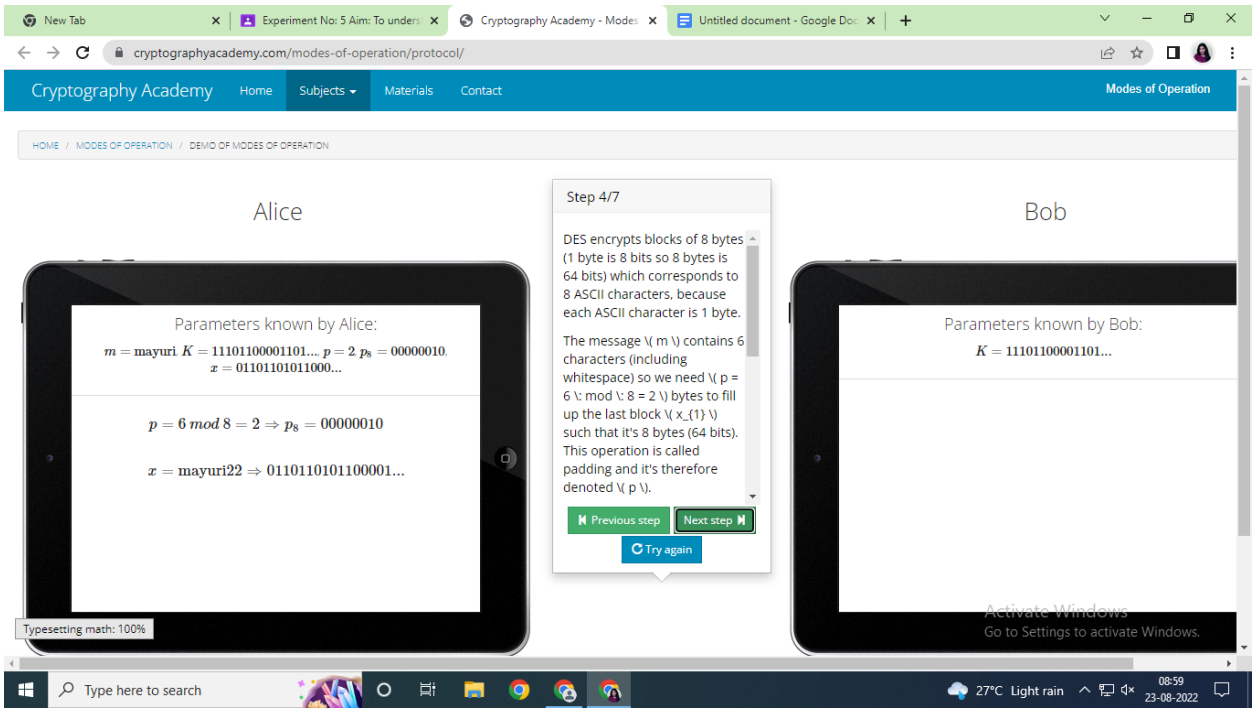

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01000011011000...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$, $IV = 00011101000011...$,
$y = 00011101000011.....$
Typesetting math: 100%
Step 7/7
Bob converts the first byte $b_1 = 01101101$ in the block x to its integer representation 109 and then to its letter representation m.
Then he converts the rest of the bytes in the block x.
Because the decimal value of the last byte $p_8 = 00000010$ in the last block x_1 is $p = 2$ and between 1 and 7, Bob know that the padding byte p_8 has been added 2 times at the end of the last block x_1.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01000011011000...$, $IV = 00011101000011...$,
$y = 00011101000011.....$, $x = 01101101011000...$, $p_8 = 00000010$,
$p = 2$, $m = \text{mayuri}$
$p_8 = 00000010 \Rightarrow p = 2$
$x = 0110110101100001... \Rightarrow \text{mayuri22}$
$m = \text{mayuri}$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:58
23-08-2022

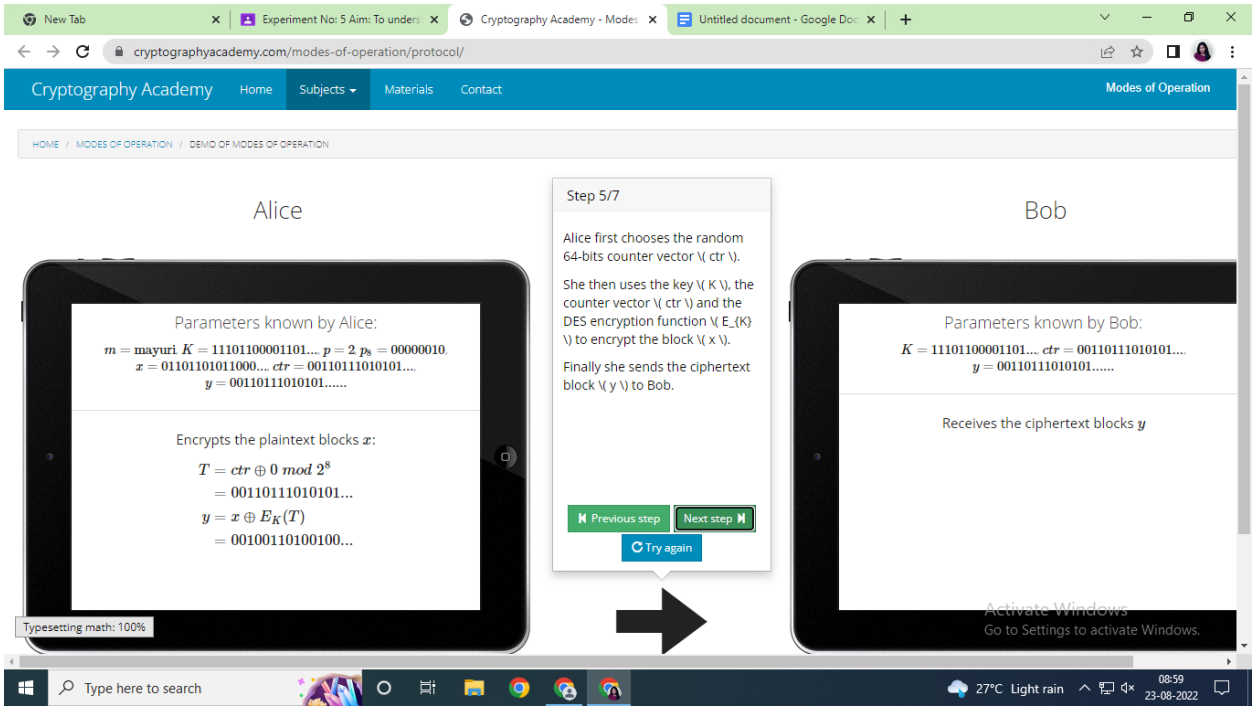
5) DES - CTR

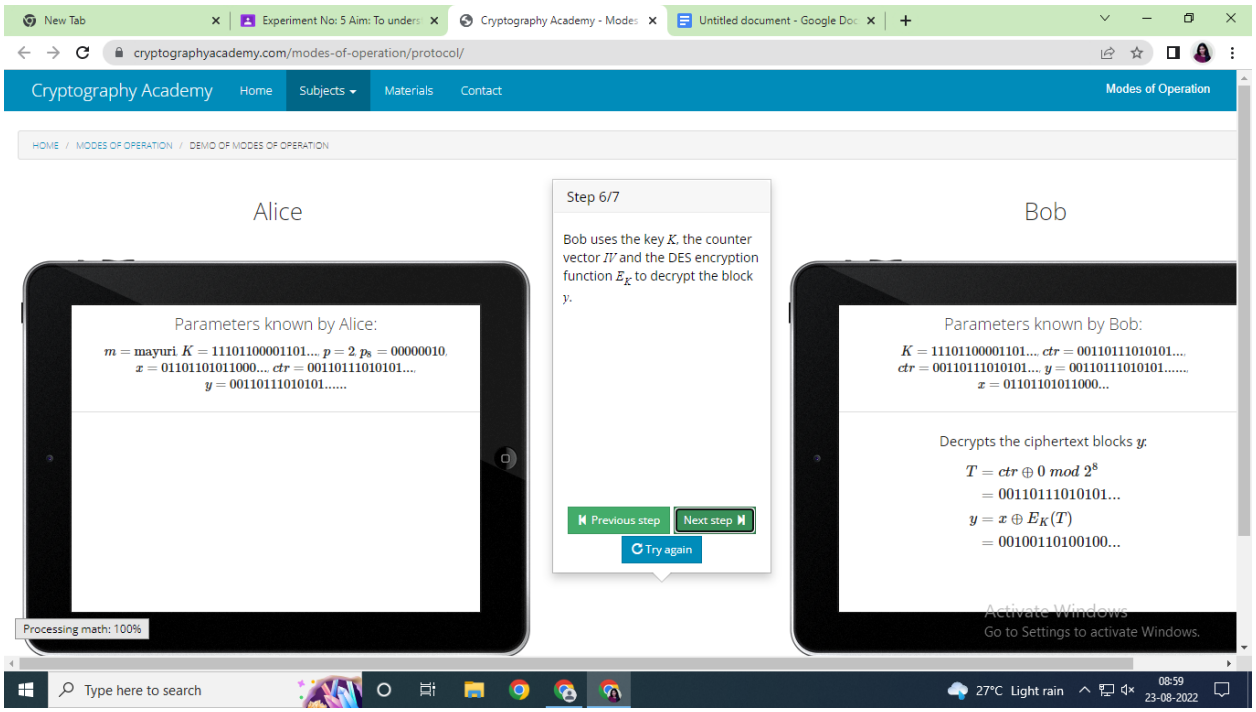

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 1/7
Enter the message (or integer) that Alice wants to send encrypted to Bob:
mayuri
Use the following cryptosystem:
The Data Encryption Standar
With the following mode of operation:
Counter (CTR) mode
Previous step
Next step
Try again
Bob
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:59
23-08-2022

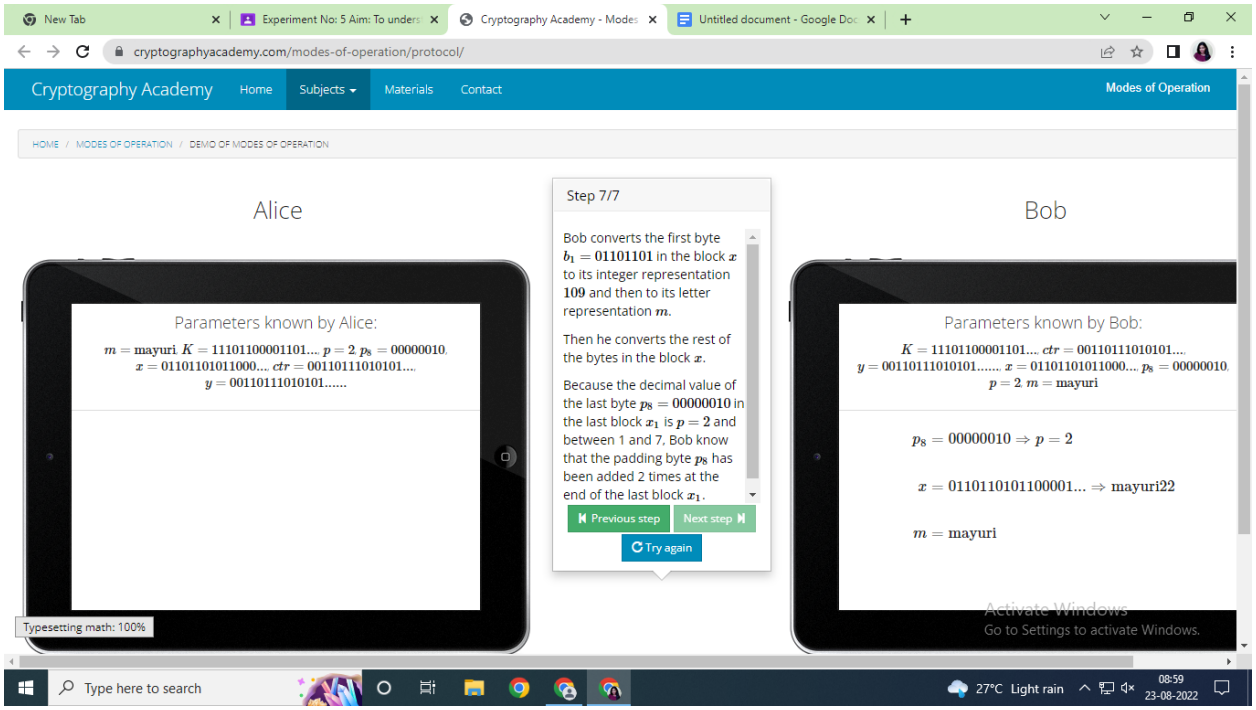

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 11101100001101...$
Chooses the key K
$K = 11101100001101...$
Step 2/7
Alice chooses the 56-bit key K for the message m.
She then sends the key K through a secure channel to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11101100001101...$
Receives the key K
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:59
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 11101100001101...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 11101100001101...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:59
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 4/7
DES encrypts blocks of 8 bytes (1 byte is 8 bits so 8 bytes is 64 bits) which corresponds to 8 ASCII characters, because each ASCII character is 1 byte.
The message \(m \) contains 6 characters (including whitespace) so we need \(p = 6 \: mod \: 8 = 2 \) bytes to fill up the last block \(x_{1} \) such that it's 8 bytes (64 bits). This operation is called padding and it's therefore denoted \(p \).
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 11101100001101...$ $p = 2$ $p_8 = 00000010$
$x = 01101101011000...$
$p = 6 \: mod \: 8 = 2 \Rightarrow p_8 = 00000010$
$x = \text{mayuri22} \Rightarrow 01101101011000001...$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 11101100001101...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:59
23-08-2022

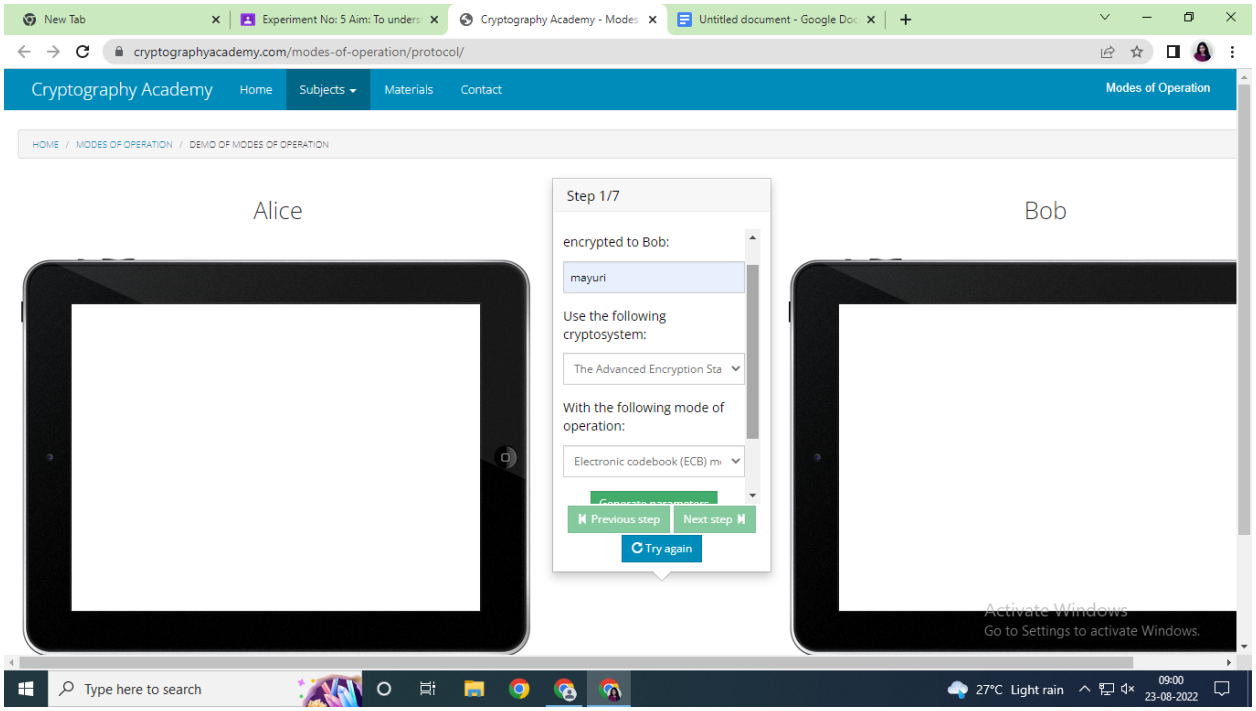

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 5/7
Alice first chooses the random 64-bits counter vector \(ctr \).
She then uses the key \(K \), the counter vector \(ctr \) and the DES encryption function \(E_{K} \) to encrypt the block \(x \).
Finally she sends the ciphertext block \(y \) to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 11101100001101...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$, $ctr = 00110111010101...$,
$y = 00110111010101.....$
Encrypts the plaintext blocks x:
$T = ctr \oplus 0 \ mod \ 2^8$
$= 00110111010101...$
$y = x \oplus E_K(T)$
$= 00100110100100...$
Parameters known by Bob:
$K = 11101100001101...$, $ctr = 00110111010101...$,
$y = 00110111010101.....$
Receives the ciphertext blocks y
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:59
23-08-2022

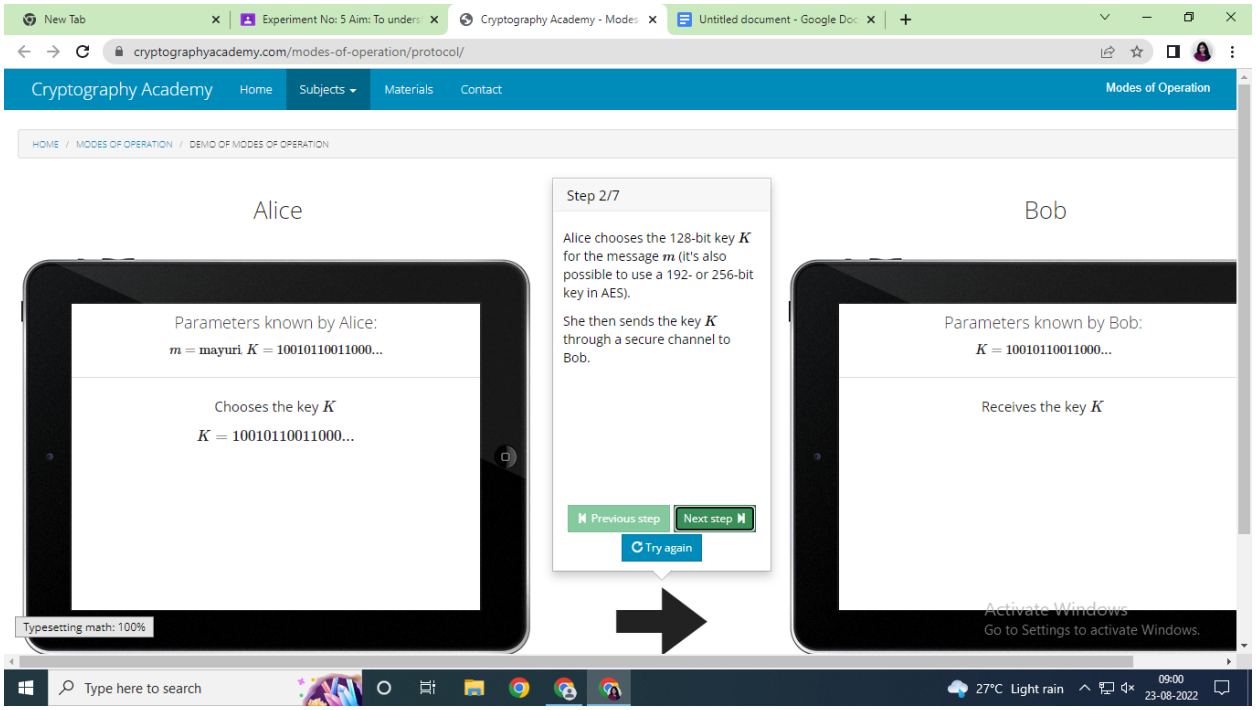

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 6/7
Bob uses the key K, the counter vector IV and the DES encryption function E_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 11101100001101...$, $p = 2$, $p_8 = 00000010$,
$x = 01101101011000...$, $ctr = 00110111010101...$,
$y = 00110111010101.....$
Parameters known by Bob:
$K = 11101100001101...$, $ctr = 00110111010101...$,
$ctr = 00110111010101...$, $y = 00110111010101.....$
$x = 01101101011000...$
Decrypts the ciphertext blocks y:
$T = ctr \oplus 0 \ mod \ 2^8$
$= 00110111010101...$
$y = x \oplus E_K(T)$
$= 00100110100100...$
Processing math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
08:59
23-08-2022

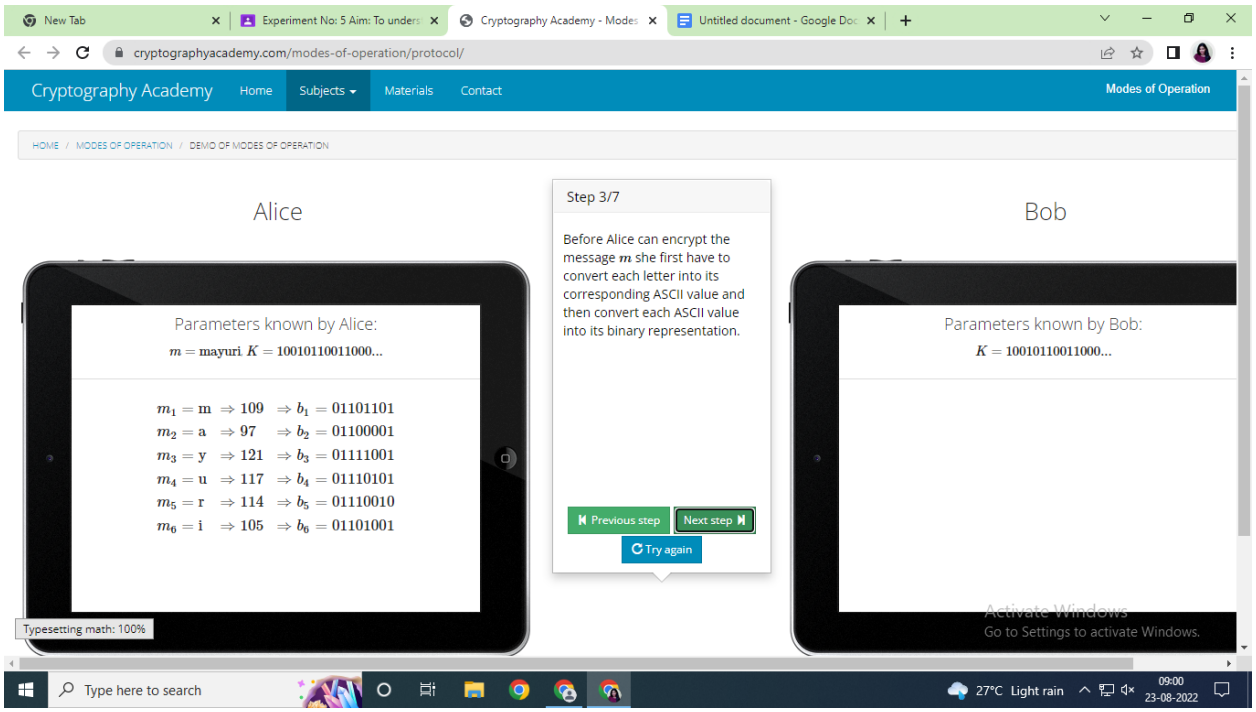


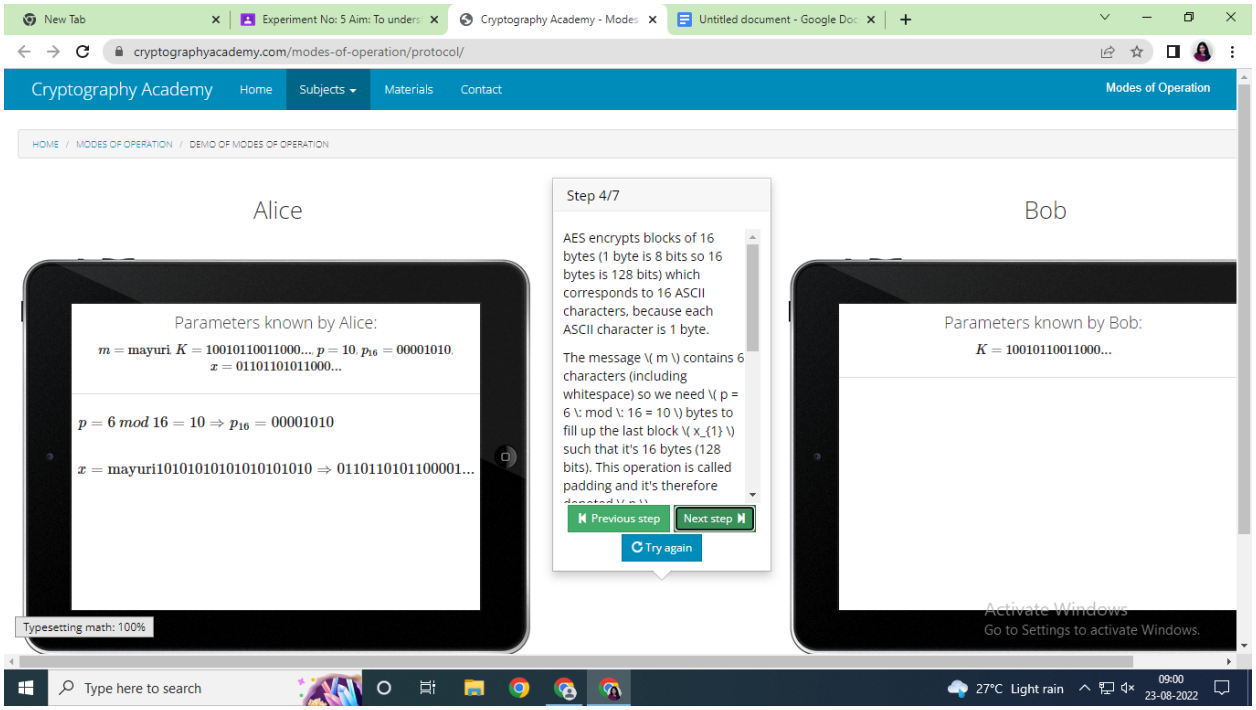
B) AES

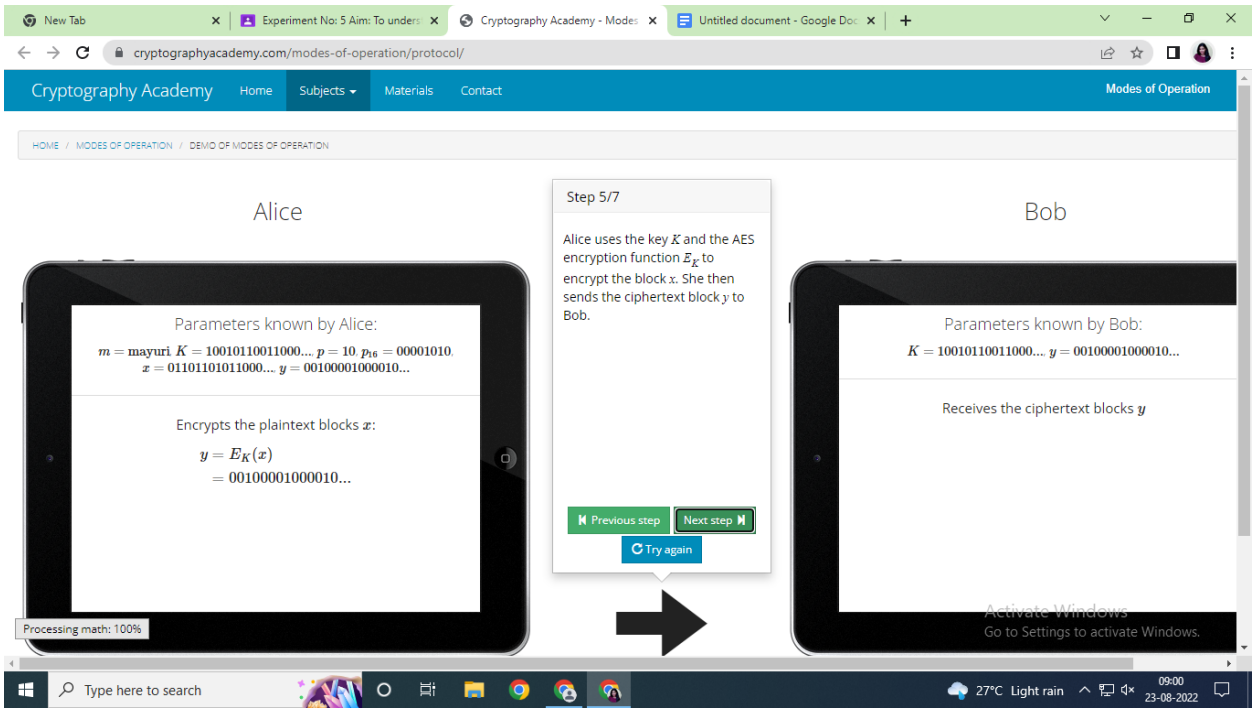
1) AES- ECB

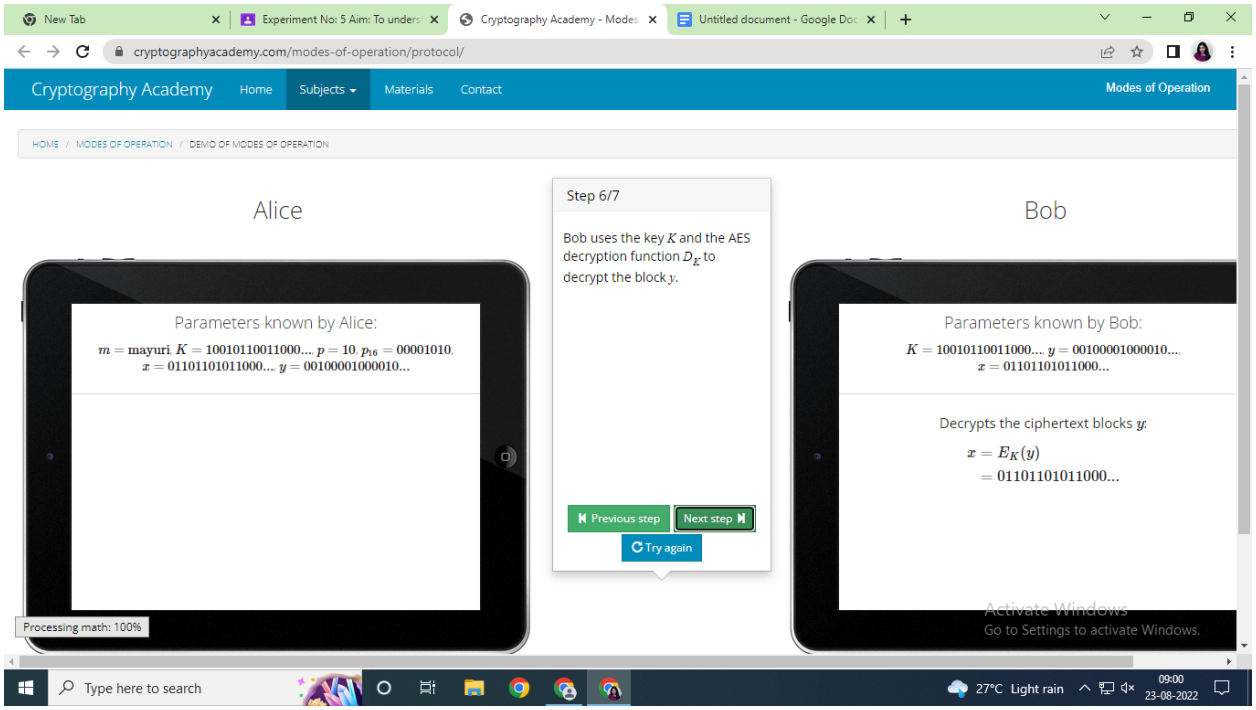


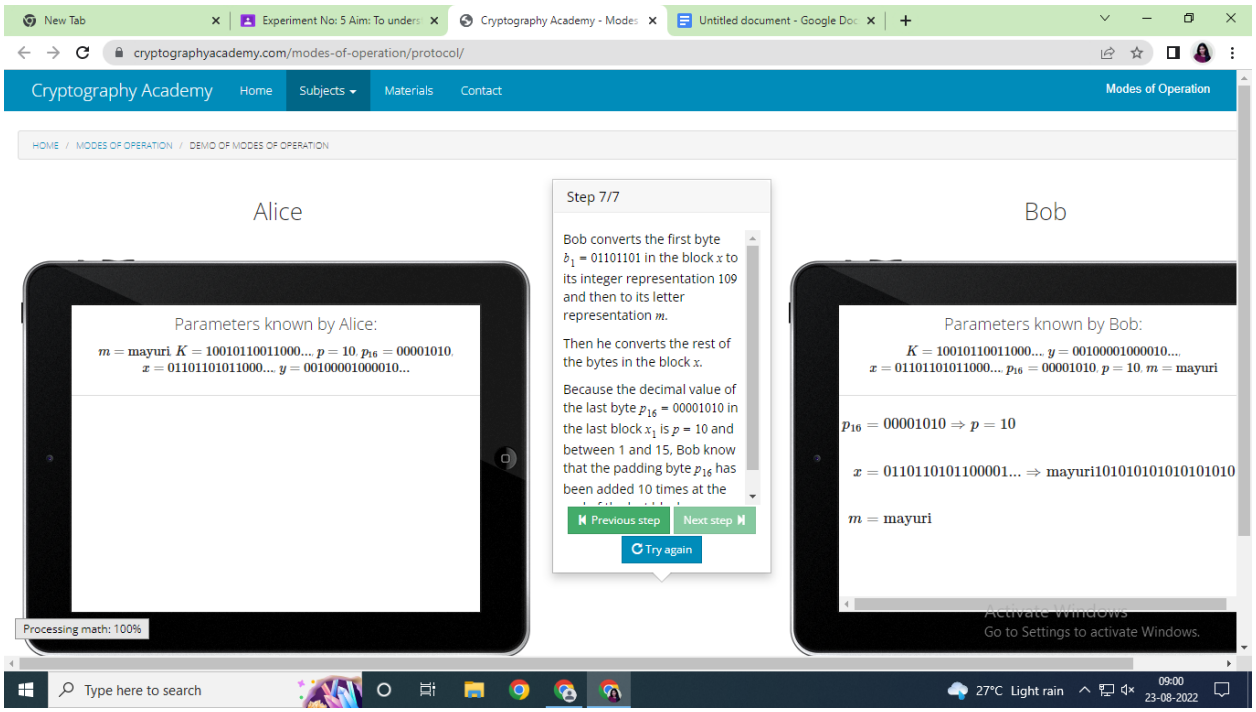

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 2/7
Alice chooses the 128-bit key K for the message m (it's also possible to use a 192- or 256-bit key in AES).
She then sends the key K through a secure channel to Bob.
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 10010110011000...$
Chooses the key K
$K = 10010110011000...$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 10010110011000...$
Receives the key K
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:00
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 10010110011000...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 10010110011000...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:00
23-08-2022

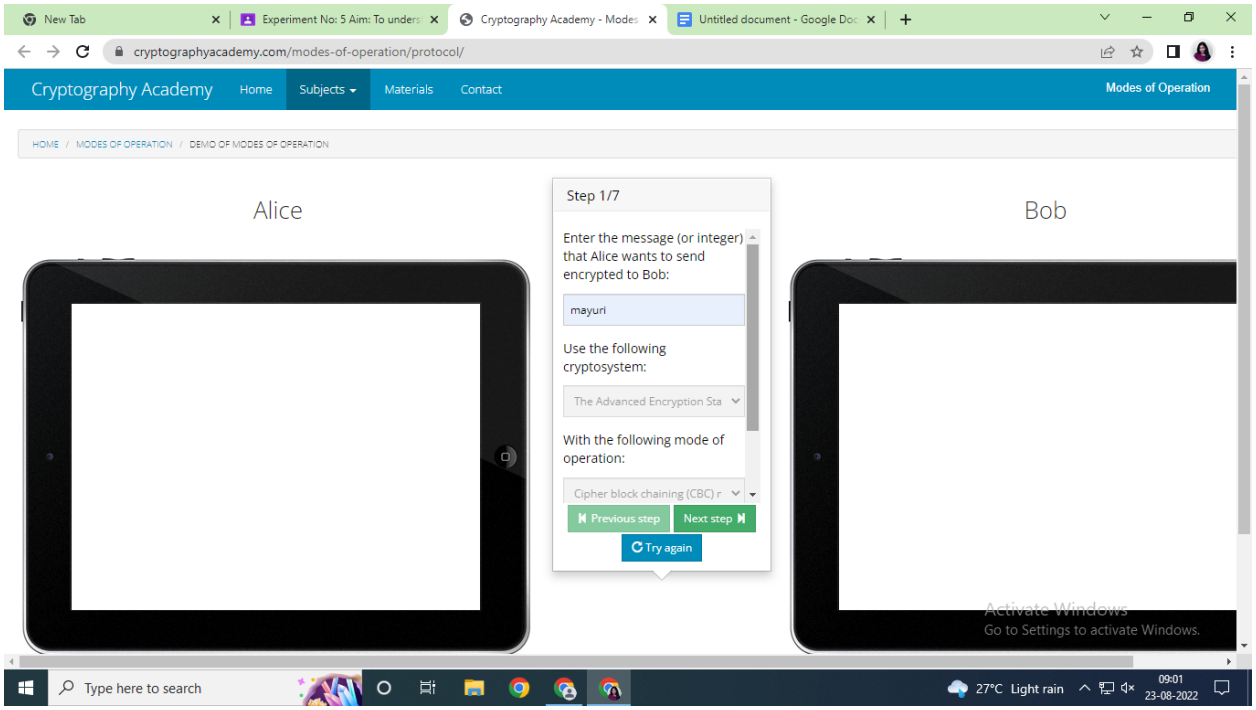

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 4/7
AES encrypts blocks of 16 bytes (1 byte is 8 bits so 16 bytes is 128 bits) which corresponds to 16 ASCII characters, because each ASCII character is 1 byte.
The message \(m \) contains 6 characters (including whitespace) so we need \(p = 6 \: mod \: 16 = 10 \) bytes to fill up the last block \(x_{1} \) such that it's 16 bytes (128 bits). This operation is called padding and it's therefore
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 10010110011000...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$
$p = 6 \; mod \; 16 = 10 \Rightarrow p_{16} = 00001010$
$x = \text{mayuri}1010101010101010101010 \Rightarrow 0110110101100001...$
Parameters known by Bob:
$K = 10010110011000...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:00
23-08-2022

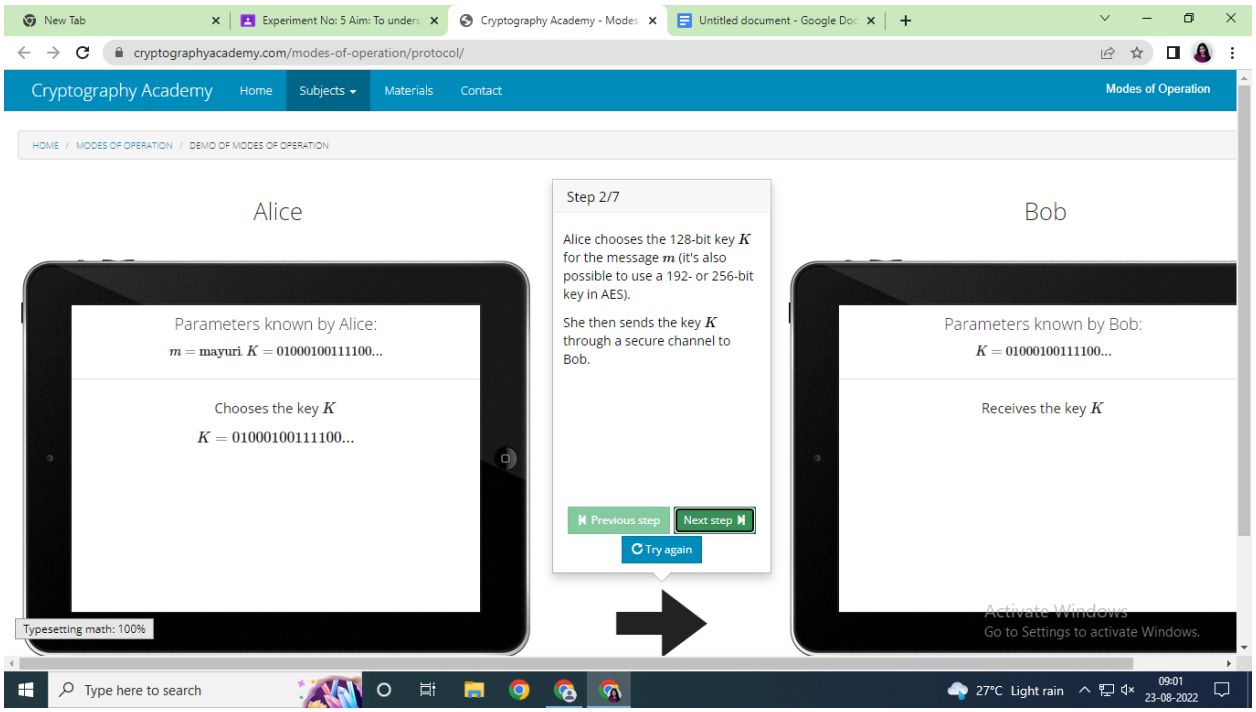

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 5/7
Alice uses the key K and the AES encryption function E_K to encrypt the block x. She then sends the ciphertext block y to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 10010110011000...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$, $y = 00100001000010...$
Encrypts the plaintext blocks x:
$y = E_K(x)$
$= 00100001000010...$
Parameters known by Bob:
$K = 10010110011000...$, $y = 00100001000010...$
Receives the ciphertext blocks y
Processing math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:00
23-08-2022

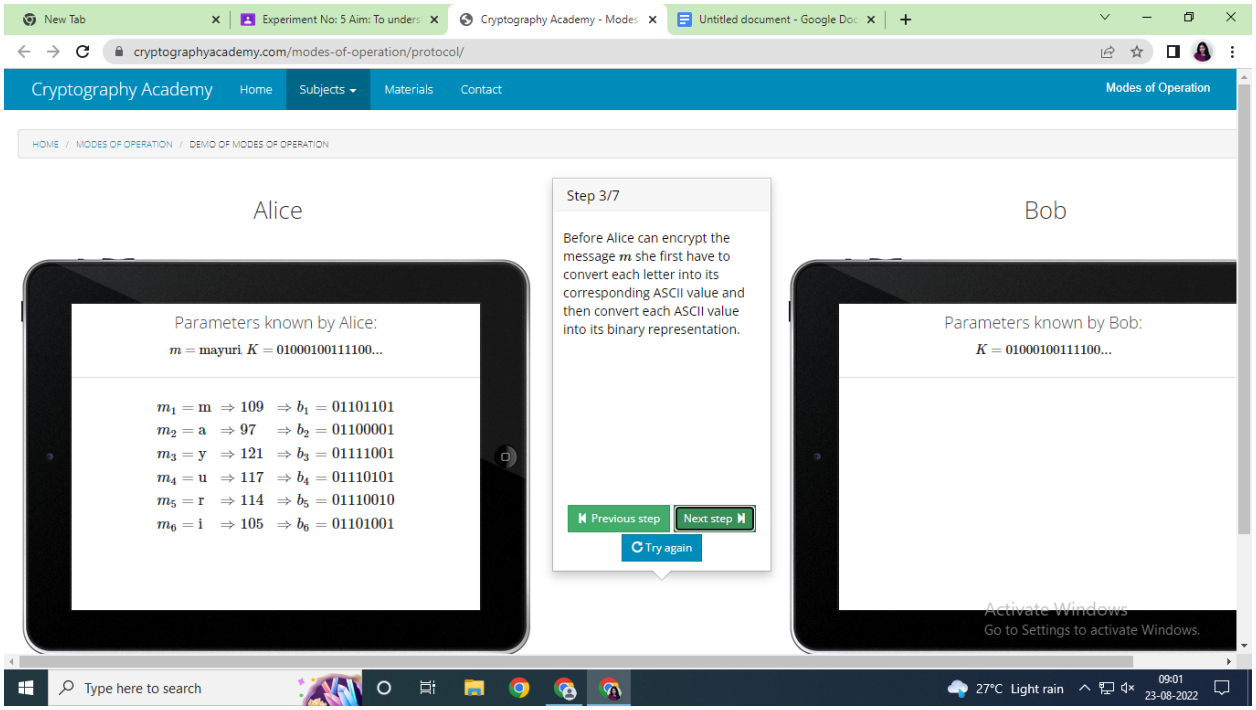

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 10010110011000...$, $p = 10$, $p_{16} = 00001010$,
$x = 01101101011000...$, $y = 00100001000010...$
Processing math: 100%
Step 6/7
Bob uses the key K and the AES decryption function D_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10010110011000...$, $y = 00100001000010...$,
$x = 01101101011000...$
Decrypts the ciphertext blocks y:
$x = E_K(y)$
$= 01101101011000...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:00
23-08-2022

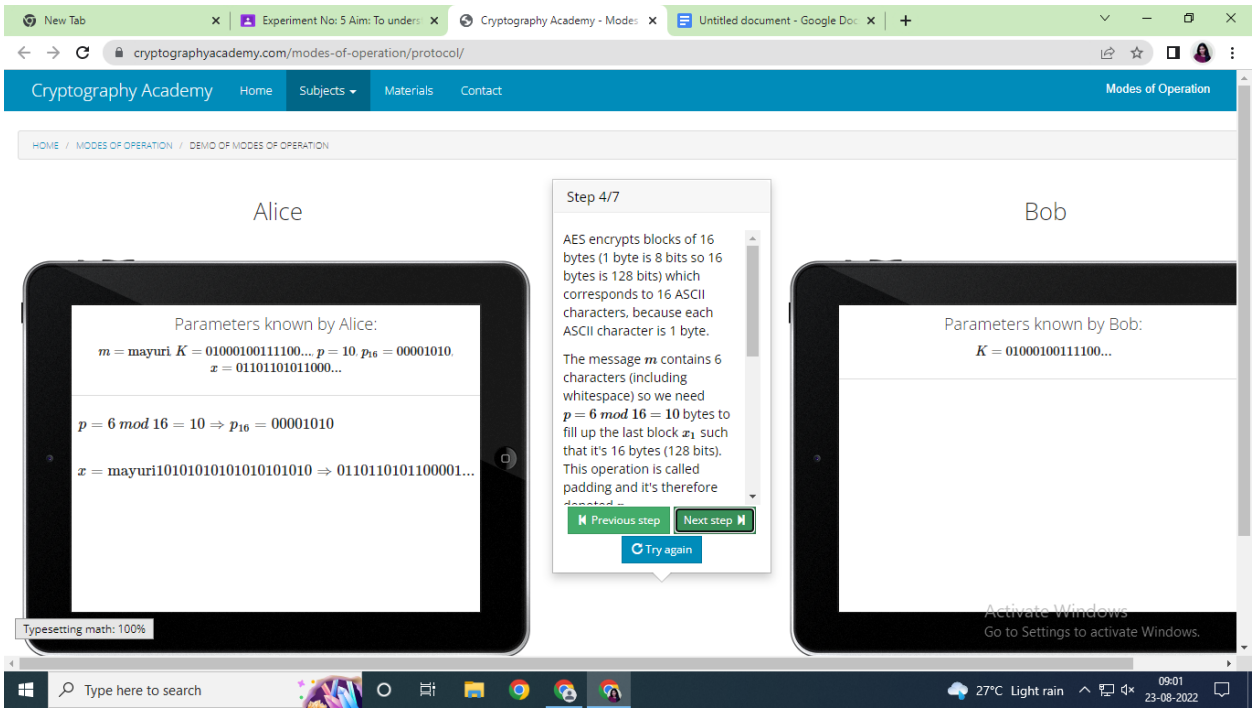

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 10010110011000...$, $p = 10$, $p_{16} = 00001010$,
$x = 01101101011000...$, $y = 00100001000010...$
Processing math: 100%
Step 7/7
Bob converts the first byte b_1 = 01101101 in the block x to its integer representation 109 and then to its letter representation m.
Then he converts the rest of the bytes in the block x.
Because the decimal value of the last byte p_{16} = 00001010 in the last block x_1 is p = 10 and between 1 and 15, Bob know that the padding byte p_{16} has been added 10 times at the
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10010110011000...$, $y = 00100001000010...$,
$x = 01101101011000...$, $p_{16} = 00001010$, $p = 10$, $m = \text{mayuri}$
$p_{16} = 00001010 \Rightarrow p = 10$
$x = 0110110101100001... \Rightarrow \text{mayuri}10101010101010101010$
$m = \text{mayuri}$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:00
23-08-2022

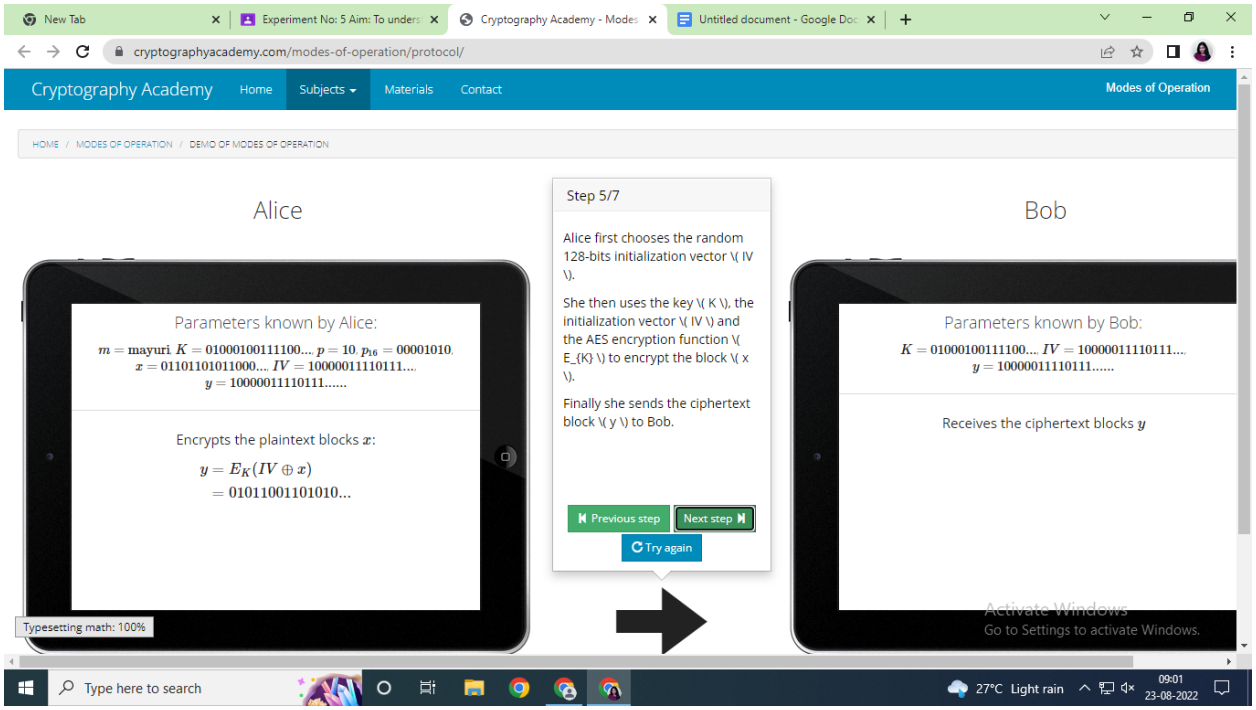
2) AES - CBC

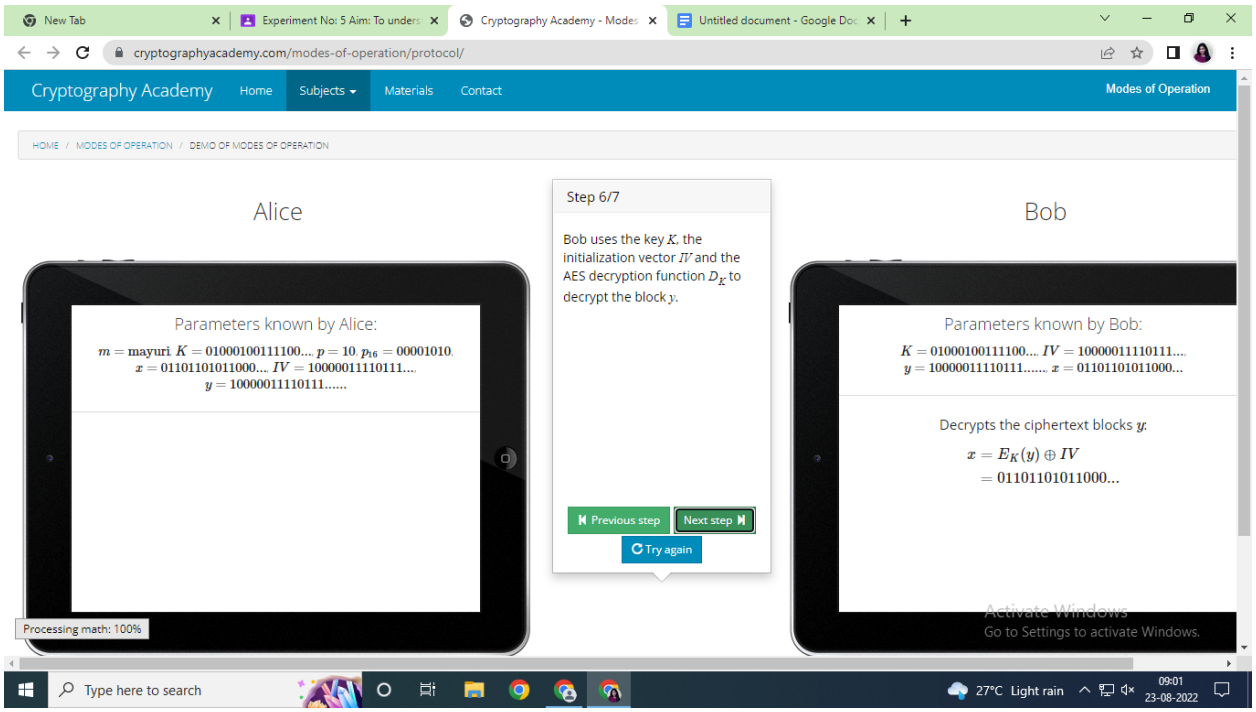

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 1/7
Enter the message (or integer) that Alice wants to send encrypted to Bob:
mayuri
Use the following cryptosystem:
The Advanced Encryption Sta
With the following mode of operation:
Cipher block chaining (CBC) r
Previous step
Next step
Try again
Bob
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:01
23-08-2022

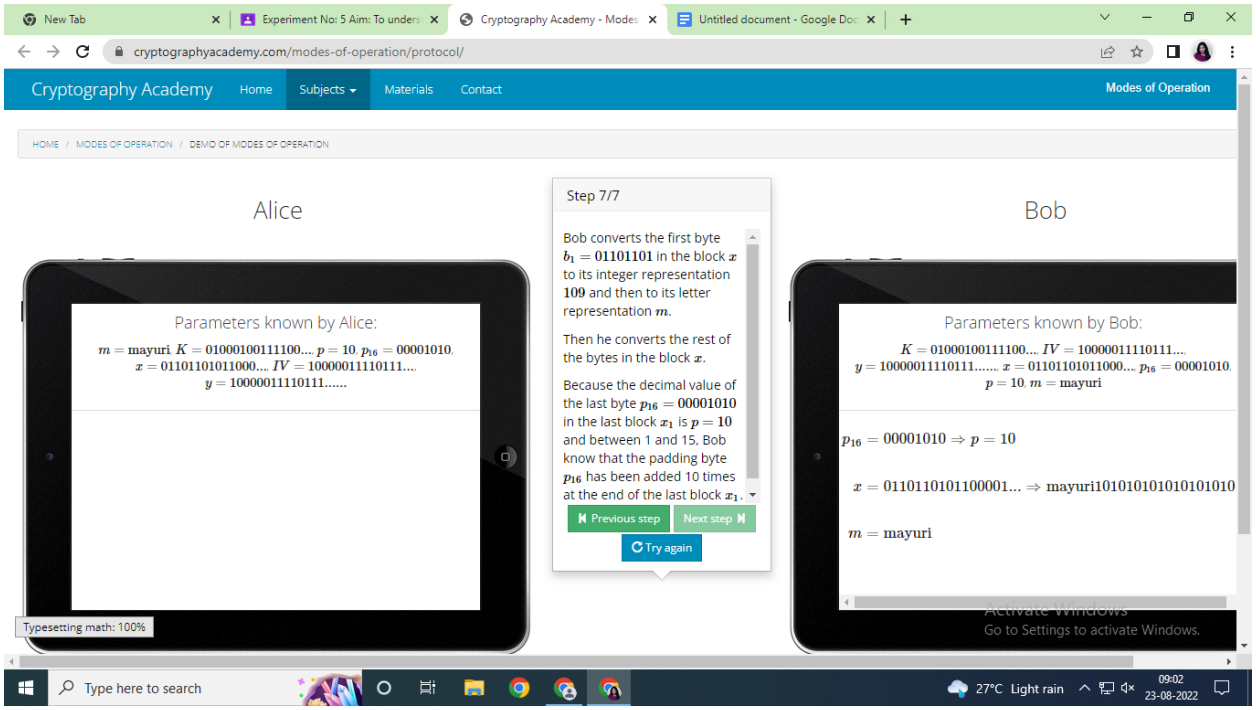

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 01000100111100...$
Chooses the key K
$K = 01000100111100...$
Typesetting math: 100%
Step 2/7
Alice chooses the 128-bit key K for the message m (it's also possible to use a 192- or 256-bit key in AES).
She then sends the key K through a secure channel to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01000100111100...$
Receives the key K
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:01
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 01000100111100...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 01000100111100...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:01
23-08-2022

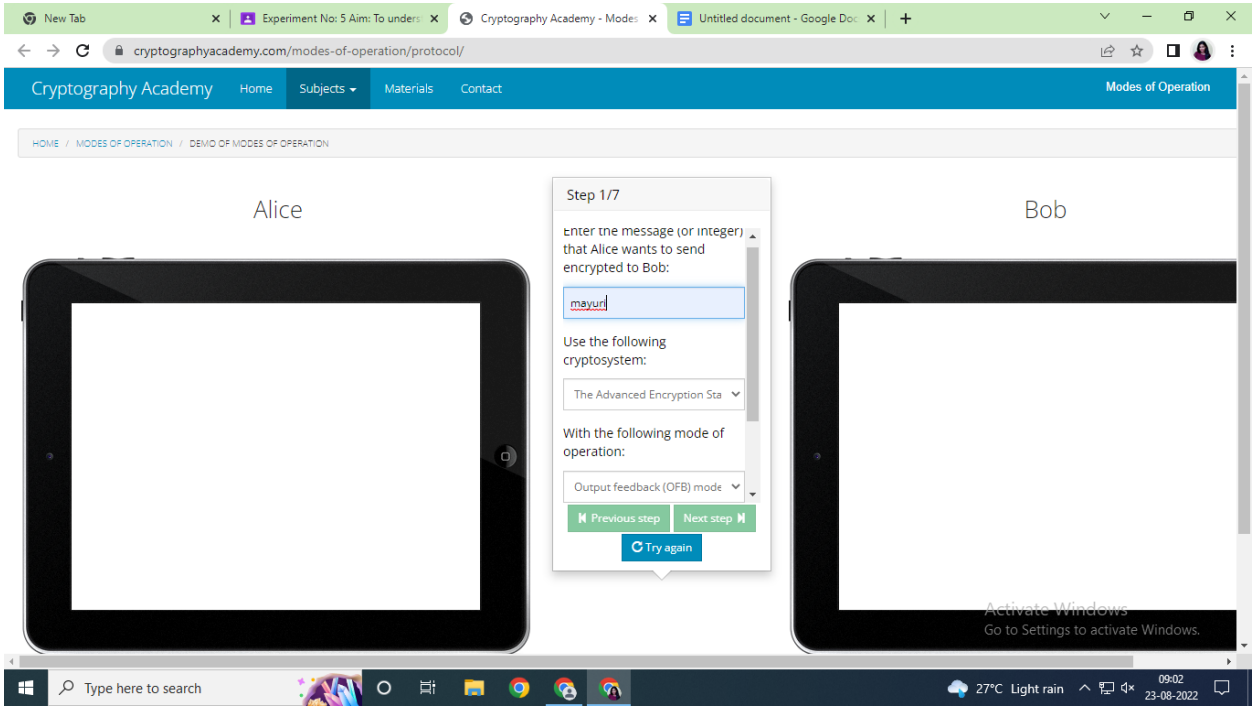

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 4/7
AES encrypts blocks of 16 bytes (1 byte is 8 bits so 16 bytes is 128 bits) which corresponds to 16 ASCII characters, because each ASCII character is 1 byte.
The message m contains 6 characters (including whitespace) so we need $p = 6 \ mod \ 16 = 10$ bytes to fill up the last block x_1 such that it's 16 bytes (128 bits). This operation is called padding and it's therefore
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 01000100111100...$ $p = 10$ $p_{16} = 00001010$ $x = 01101101011000...$
$p = 6 \ mod \ 16 = 10 \Rightarrow p_{16} = 00001010$
$x = \text{mayuri}1010101010101010101010 \Rightarrow 01101101011000001...$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 01000100111100...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:01
23-08-2022

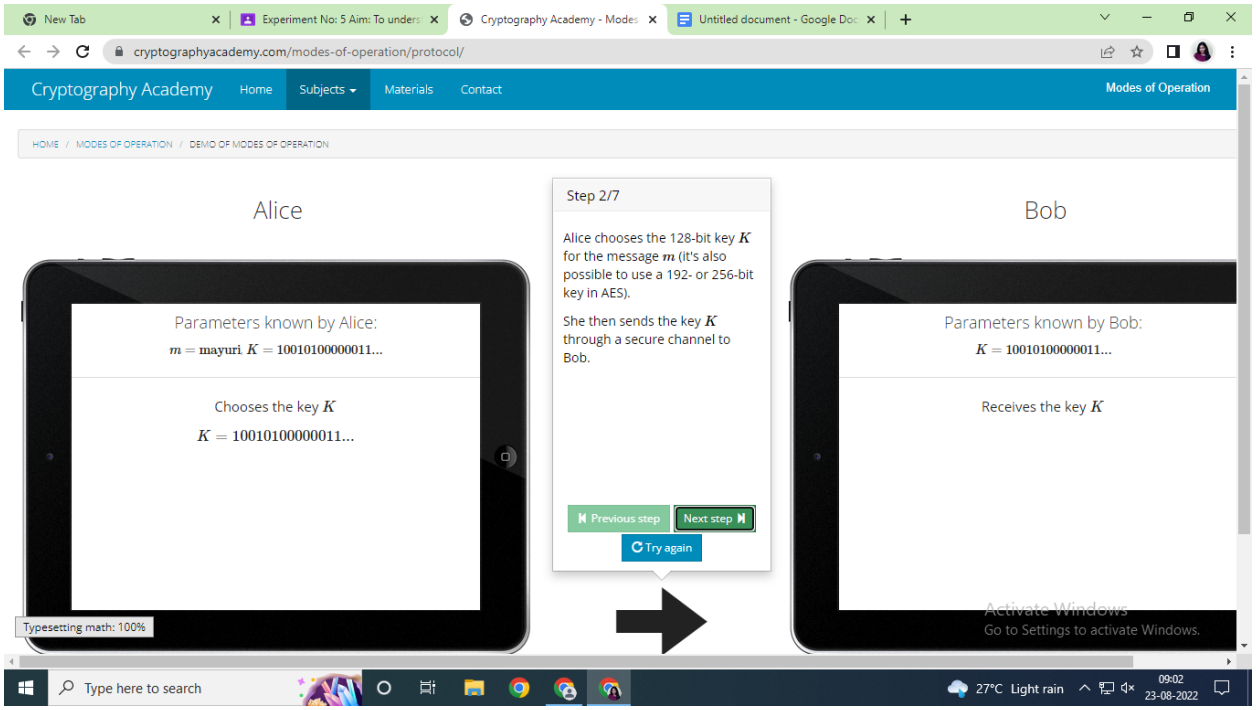

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01000100111100...$, $p = 10$, $p_{16} = 00001010$,
$x = 01101101011000...$, $IV = 10000011110111...$,
$y = 10000011110111.....$
Encrypts the plaintext blocks x:
$y = E_K(IV \oplus x)$
$= 01011001101010...$
Step 5/7
Alice first chooses the random 128-bits initialization vector \(IV \).
She then uses the key \(K \), the initialization vector \(IV \) and the AES encryption function \(E_{K} \) to encrypt the block \(x \).
Finally she sends the ciphertext block \(y \) to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01000100111100...$, $IV = 10000011110111...$,
$y = 10000011110111.....$
Receives the ciphertext blocks y
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:01
23-08-2022

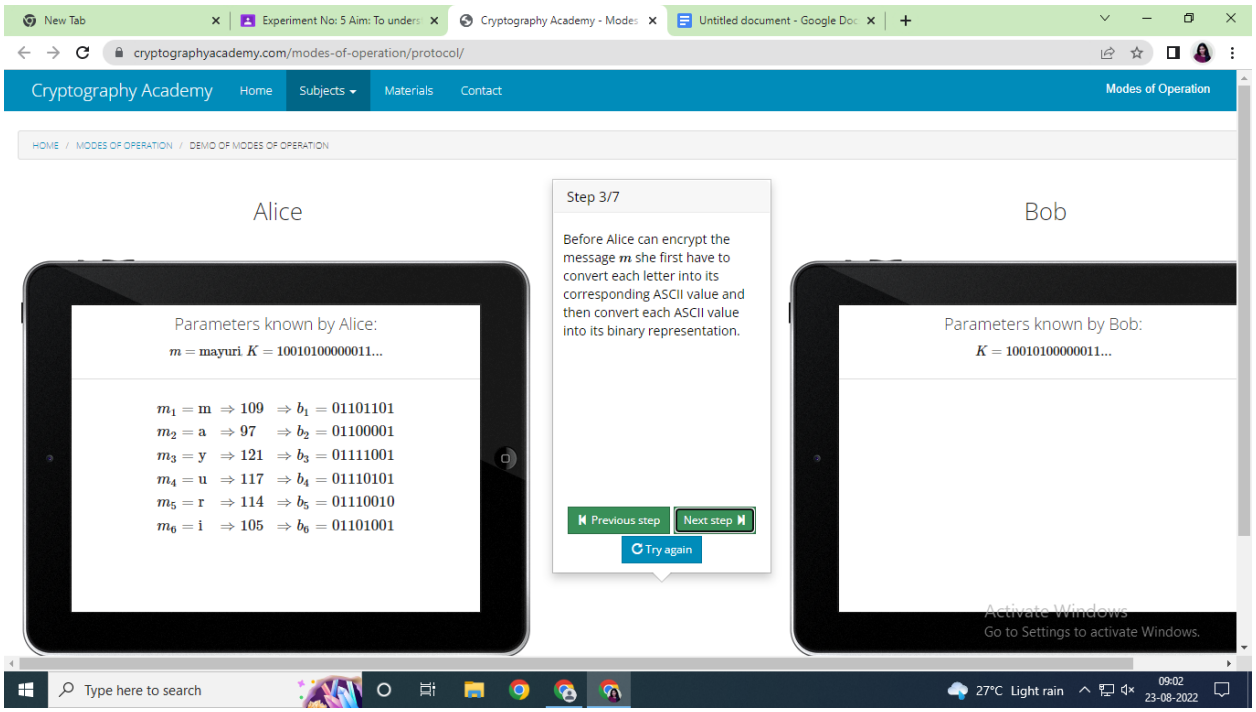

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01000100111100...$, $p = 10$, $p_{16} = 00001010$,
$x = 01101101011000...$, $IV = 10000011110111...$,
$y = 10000011110111.....$
Step 6/7
Bob uses the key K, the initialization vector IV and the AES decryption function D_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01000100111100...$, $IV = 10000011110111...$,
$y = 10000011110111.....$ $x = 01101101011000...$
Decrypts the ciphertext blocks y:
$x = E_K(y) \oplus IV$
$= 01101101011000...$
Processing math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:01
23-08-2022

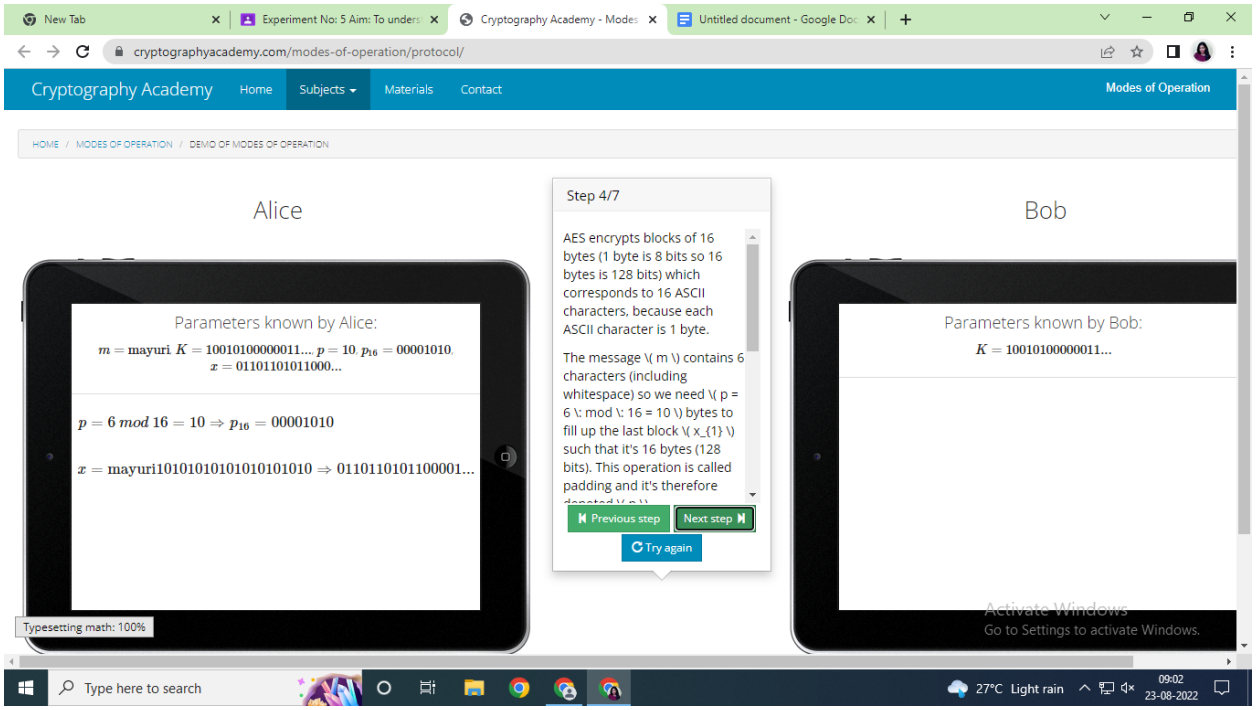

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 01000100111100...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$, $IV = 10000011110111...$, $y = 10000011110111.....$
Typesetting math: 100%
Step 7/7
Bob converts the first byte $b_1 = 01101101$ in the block x to its integer representation 109 and then to its letter representation m.
Then he converts the rest of the bytes in the block x.
Because the decimal value of the last byte $p_{16} = 00001010$ in the last block x_1 is $p = 10$ and between 1 and 15, Bob know that the padding byte p_{16} has been added 10 times at the end of the last block x_1.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 01000100111100...$, $IV = 10000011110111...$, $y = 10000011110111.....$, $x = 01101101011000...$, $p_{16} = 00001010$, $p = 10$, $m = \text{mayuri}$
$p_{16} = 00001010 \Rightarrow p = 10$
$x = 0110110101100001... \Rightarrow \text{mayuri}10101010101010101010$
$m = \text{mayuri}$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:02
23-08-2022

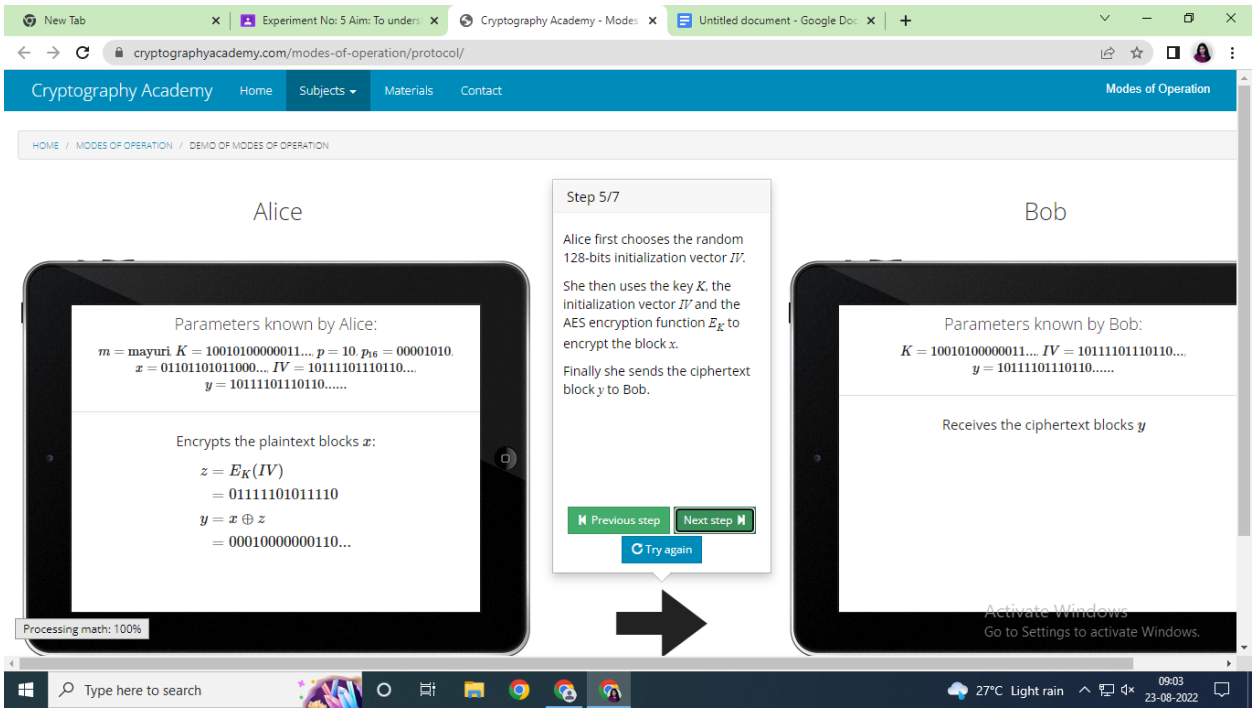
3) AES- OFB

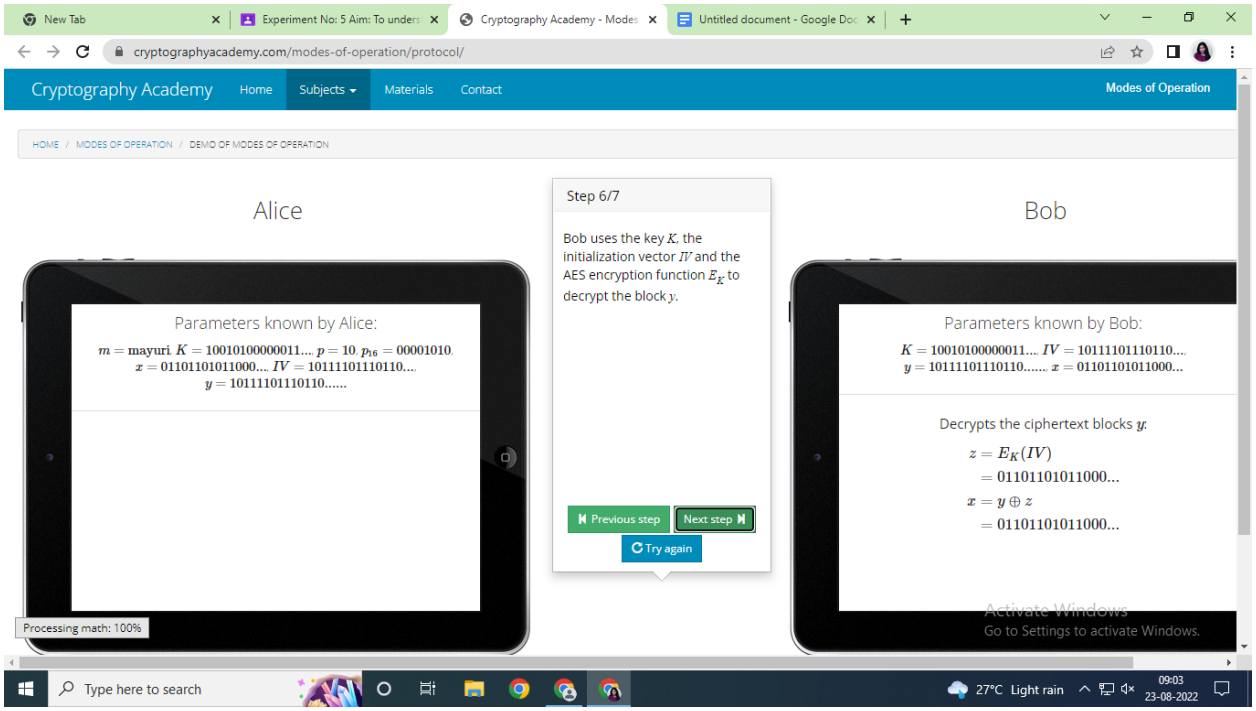

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 1/7
Enter the message (or integer) that Alice wants to send encrypted to Bob:
mayuri
Use the following cryptosystem:
The Advanced Encryption Sta
With the following mode of operation:
Output feedback (OFB) mode
Previous step
Next step
Try again
Bob
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:02
23-08-2022

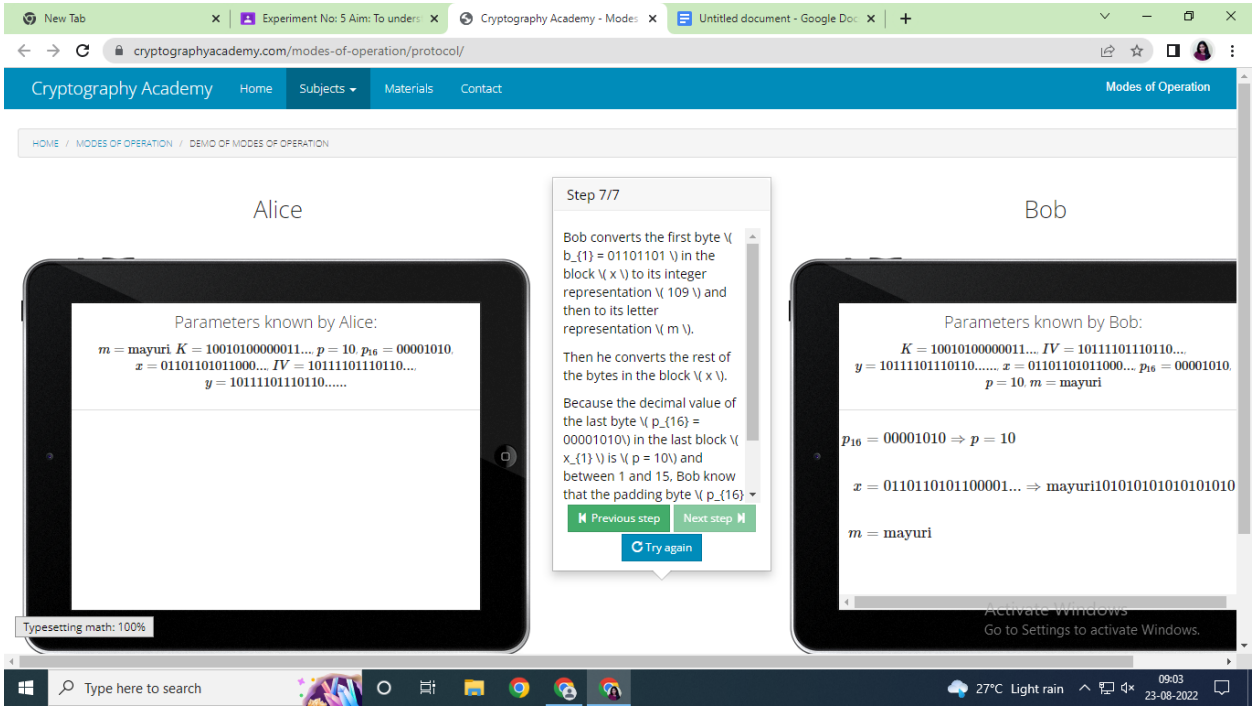

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 10010100000011...$
Chooses the key K
$K = 10010100000011...$
Step 2/7
Alice chooses the 128-bit key K for the message m (it's also possible to use a 192- or 256-bit key in AES).
She then sends the key K through a secure channel to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10010100000011...$
Receives the key K
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:02
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 10010100000011...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10010100000011...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:02
23-08-2022

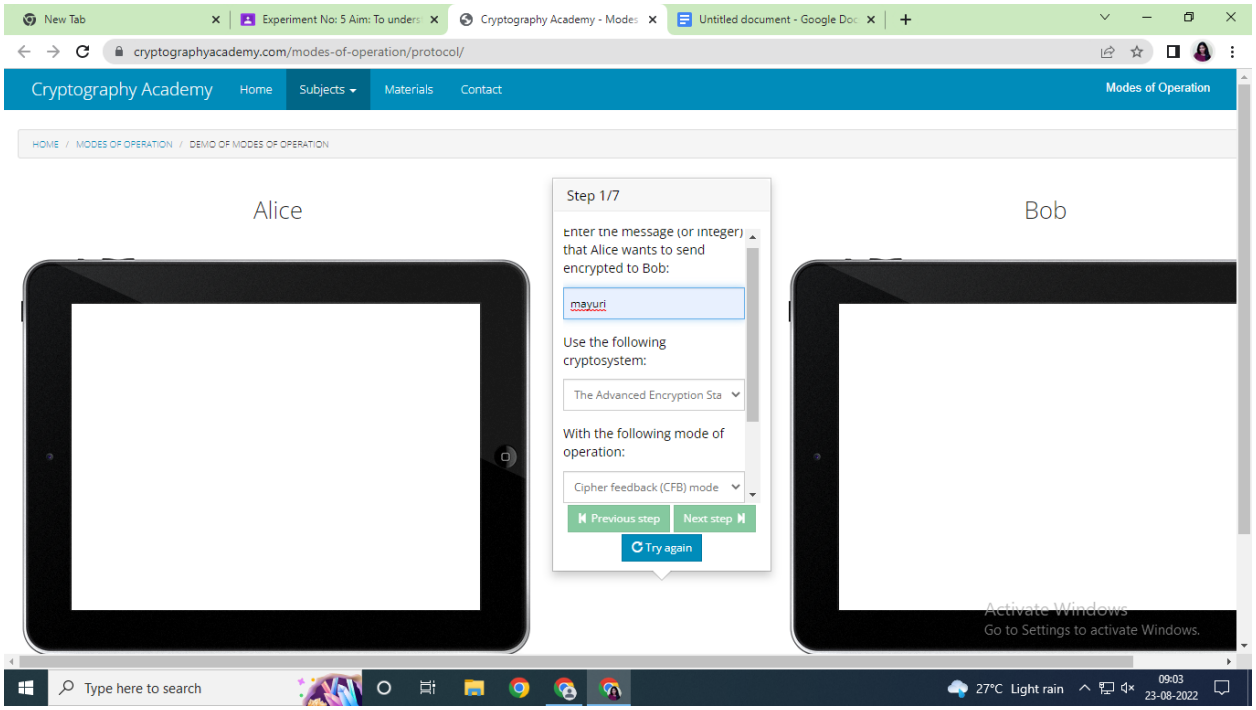

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 4/7
AES encrypts blocks of 16 bytes (1 byte is 8 bits so 16 bytes is 128 bits) which corresponds to 16 ASCII characters, because each ASCII character is 1 byte.
The message \(m \) contains 6 characters (including whitespace) so we need \(p = 6 \: mod \: 16 = 10 \) bytes to fill up the last block \(x_{1} \) such that it's 16 bytes (128 bits). This operation is called padding and it's therefore
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 10010100000011...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$
$p = 6 \; mod \; 16 = 10 \Rightarrow p_{16} = 00001010$
$x = \text{mayuri}1010101010101010101010 \Rightarrow 0110110101100001...$
Parameters known by Bob:
$K = 10010100000011...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:02
23-08-2022

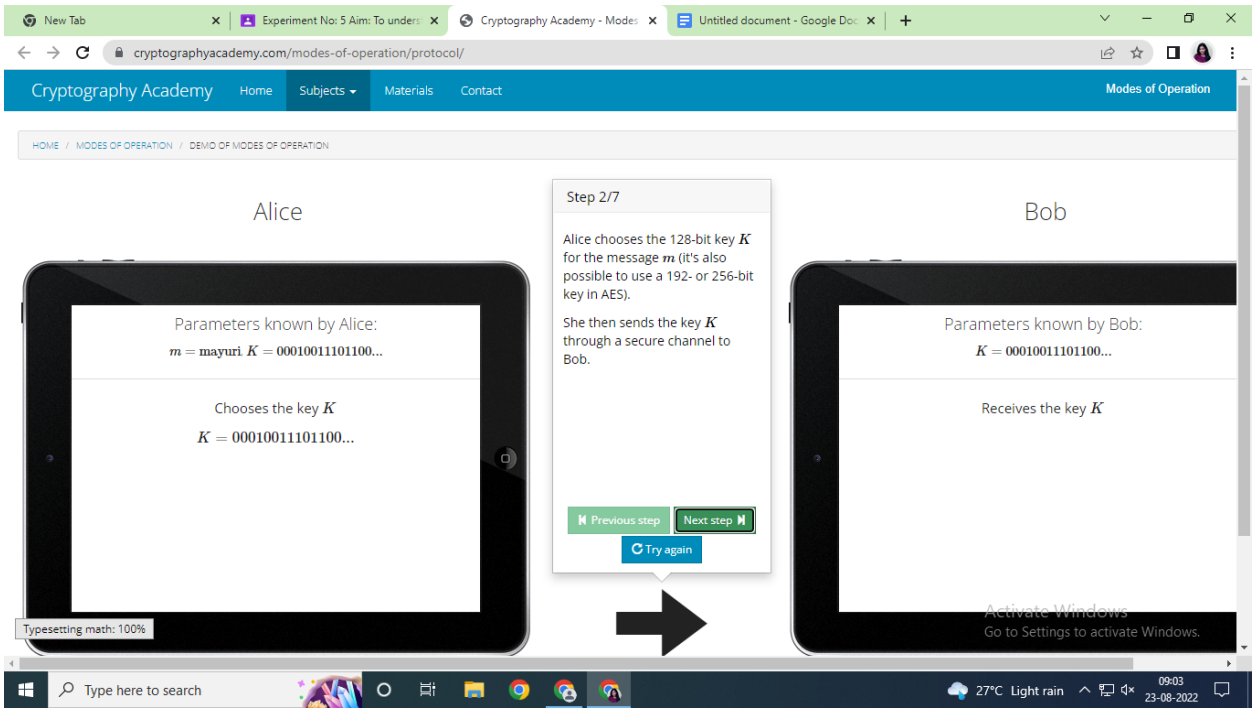

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 5/7
Alice first chooses the random 128-bits initialization vector IV.
She then uses the key K, the initialization vector IV and the AES encryption function E_K to encrypt the block x.
Finally she sends the ciphertext block y to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 10010100000011...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$, $IV = 10111101110110...$, $y = 10111101110110.....$
Encrypts the plaintext blocks x:
$z = E_K(IV)$
$= 01111101011110$
$y = x \oplus z$
$= 00010000000110...$
Parameters known by Bob:
$K = 10010100000011...$, $IV = 10111101110110...$, $y = 10111101110110.....$
Receives the ciphertext blocks y
Processing math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:03
23-08-2022

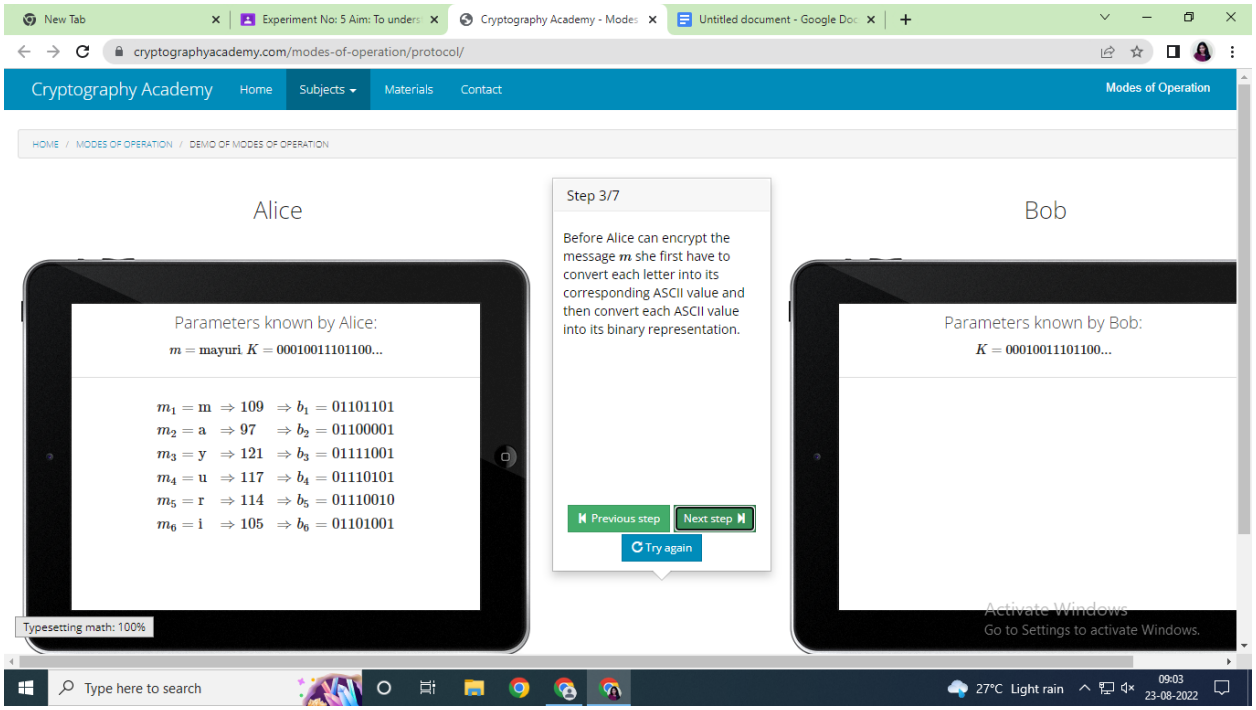

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 10010100000011...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$, $IV = 10111101110110...$, $y = 10111101110110.....$
Step 6/7
Bob uses the key K, the initialization vector IV and the AES encryption function E_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10010100000011...$, $IV = 10111101110110...$, $y = 10111101110110.....$, $x = 01101101011000...$
Decrypts the ciphertext blocks y.
$z = E_K(IV)$
$= 01101101011000...$
$x = y \oplus z$
$= 01101101011000...$
Processing math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:03
23-08-2022

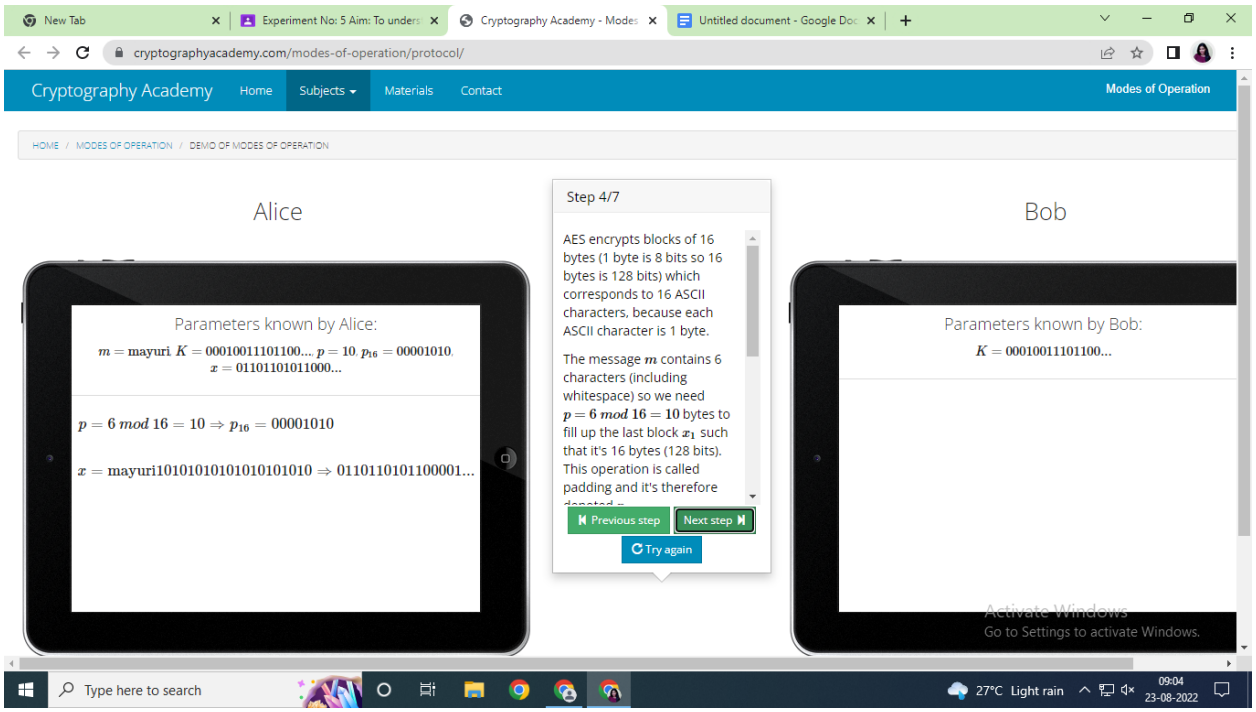

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 10010100000011...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$, $IV = 10111101110110...$, $y = 10111101110110.....$
Step 7/7
Bob converts the first byte \(b_{1} = 01101101 \) in the block \(x \) to its integer representation \(109 \) and then to its letter representation \(m \).
Then he converts the rest of the bytes in the block \(x \).
Because the decimal value of the last byte \(p_{16} = 00001010\) in the last block \(x_{1} \) is \(p = 10\) and between 1 and 15, Bob know that the padding byte \(p_{16}
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10010100000011...$, $IV = 10111101110110...$, $y = 10111101110110.....$, $x = 01101101011000...$, $p_{16} = 00001010$, $p = 10$, $m = \text{mayuri}$
$p_{16} = 00001010 \Rightarrow p = 10$
$x = 0110110101100001... \Rightarrow \text{mayuri}10101010101010101$
$m = \text{mayuri}$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:03
23-08-2022

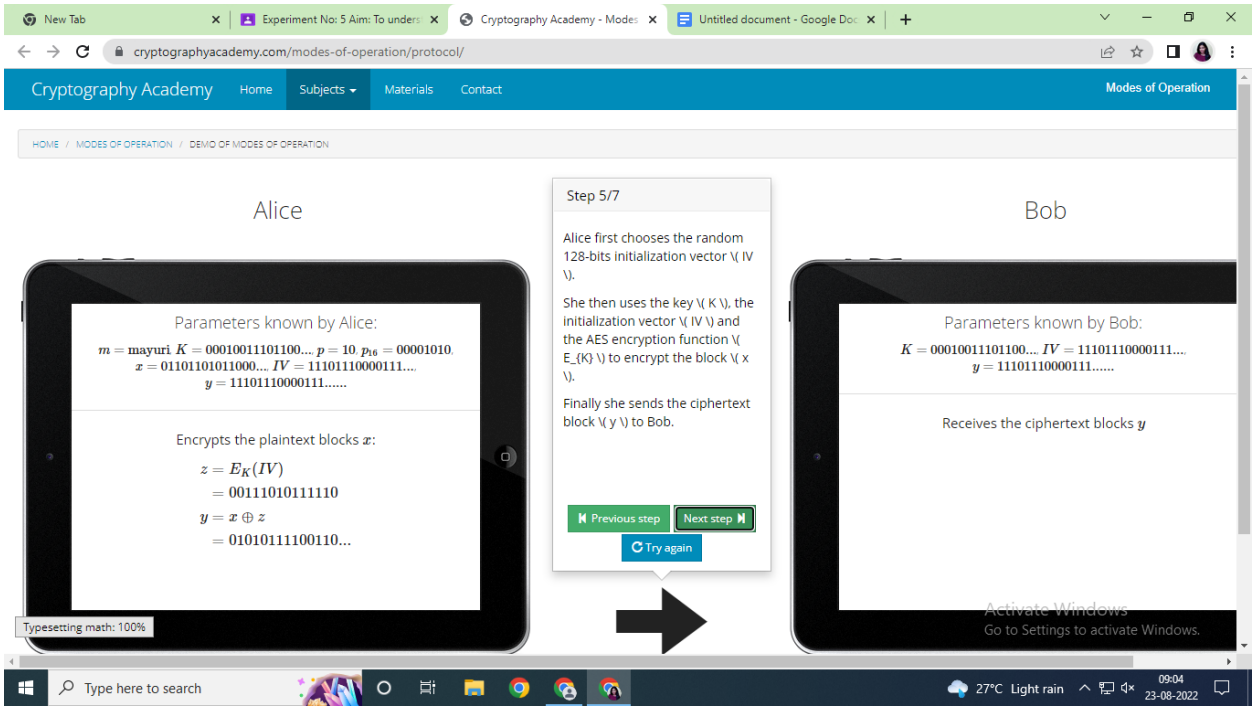
4) AES - CFB

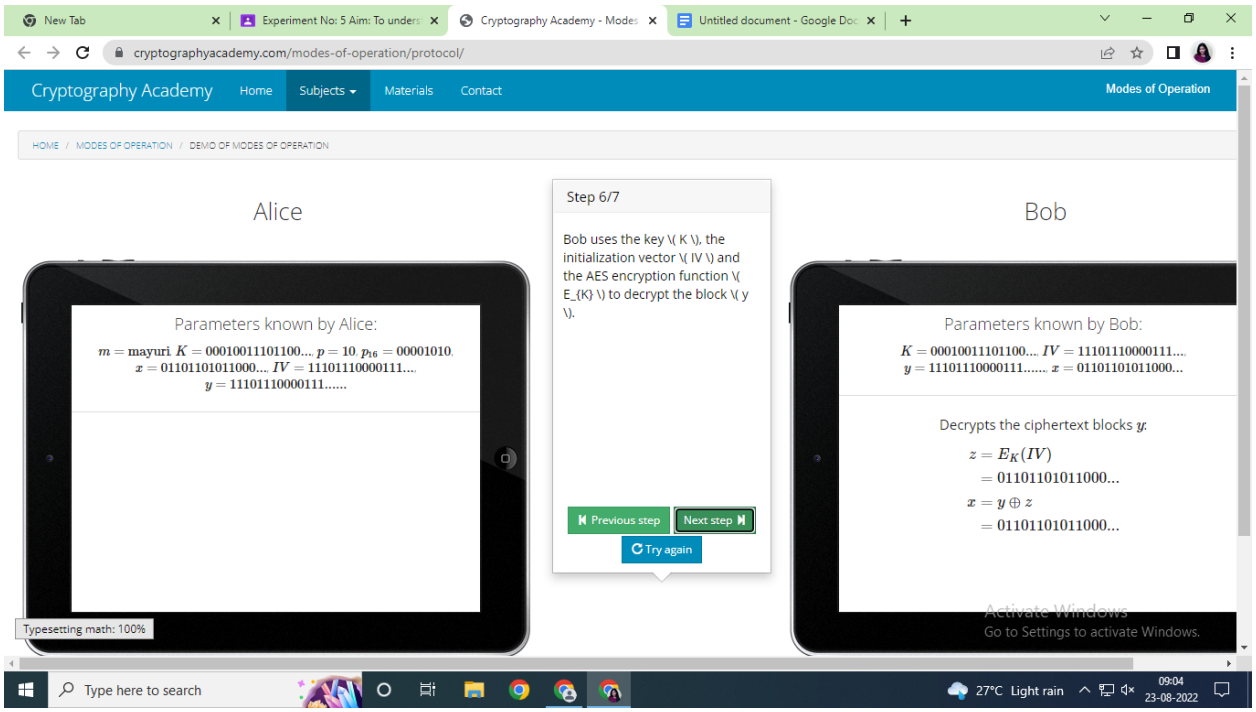

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 1/7
Enter the message (or integer) that Alice wants to send encrypted to Bob:
mayuri
Use the following cryptosystem:
The Advanced Encryption Sta
With the following mode of operation:
Cipher feedback (CFB) mode
Previous step
Next step
Try again
Bob
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:03
23-08-2022

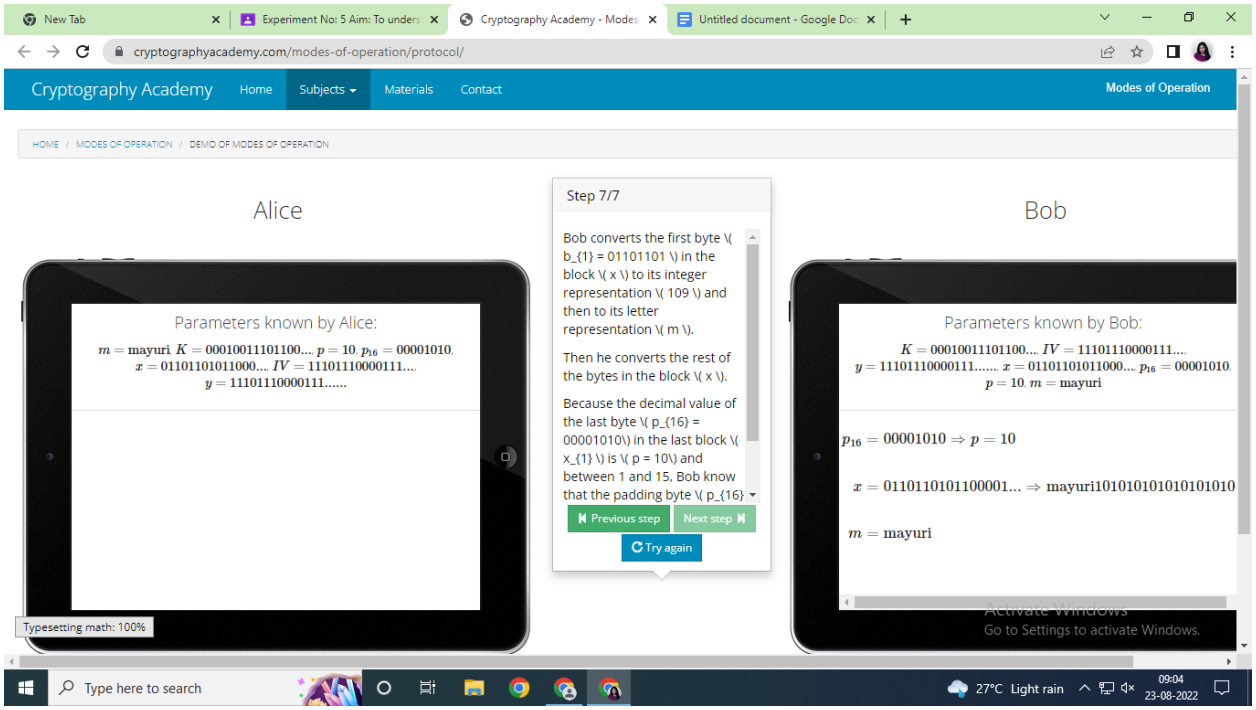

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 00010011101100...$
Chooses the key K
$K = 00010011101100...$
Typesetting math: 100%
Step 2/7
Alice chooses the 128-bit key K for the message m (it's also possible to use a 192- or 256-bit key in AES).
She then sends the key K through a secure channel to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 00010011101100...$
Receives the key K
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:03
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 00010011101100...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 00010011101100...$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:03
23-08-2022

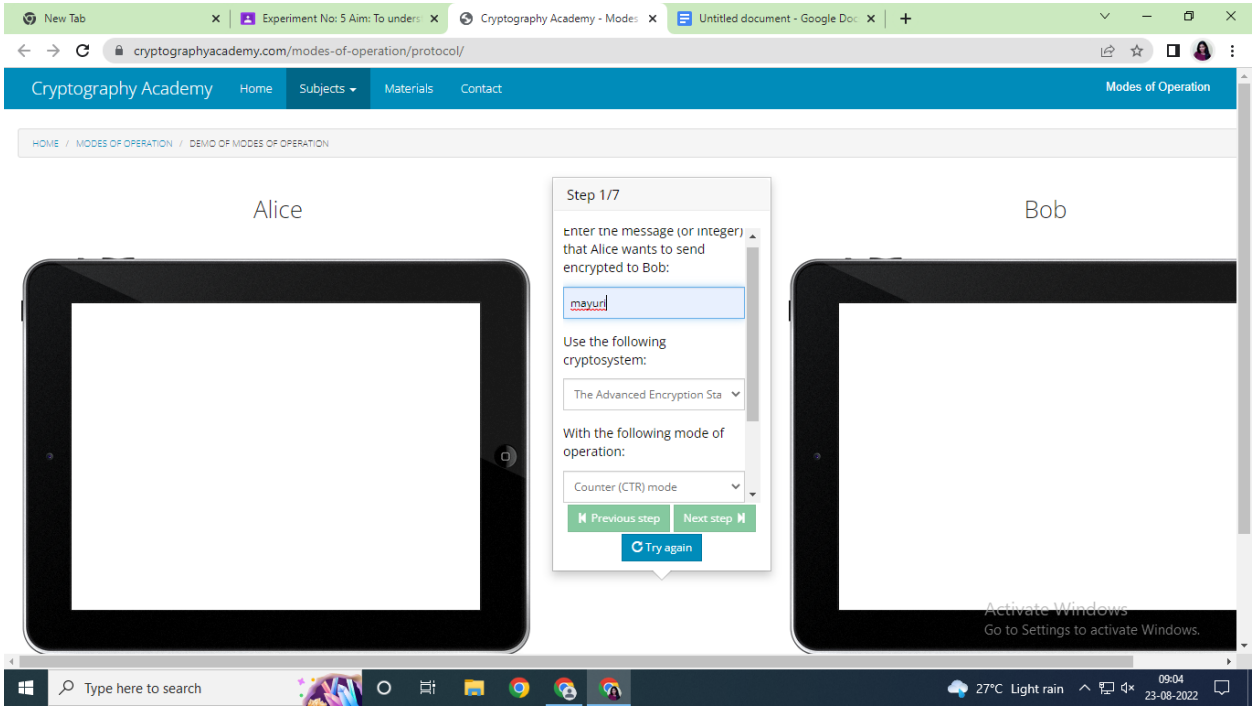

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 4/7
AES encrypts blocks of 16 bytes (1 byte is 8 bits so 16 bytes is 128 bits) which corresponds to 16 ASCII characters, because each ASCII character is 1 byte.
The message m contains 6 characters (including whitespace) so we need $p = 6 \ mod \ 16 = 10$ bytes to fill up the last block x_1 such that it's 16 bytes (128 bits). This operation is called padding and it's therefore
Bob
Parameters known by Alice:
$m = \text{mayuri}$ $K = 00010011101100...$ $p = 10$ $p_{16} = 00001010$
$x = 01101101011000...$
$p = 6 \ mod \ 16 = 10 \Rightarrow p_{16} = 00001010$
$x = \text{mayuri}1010101010101010101010 \Rightarrow 01101101011000001...$
Previous step
Next step
Try again
Parameters known by Bob:
$K = 00010011101100...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:04
23-08-2022

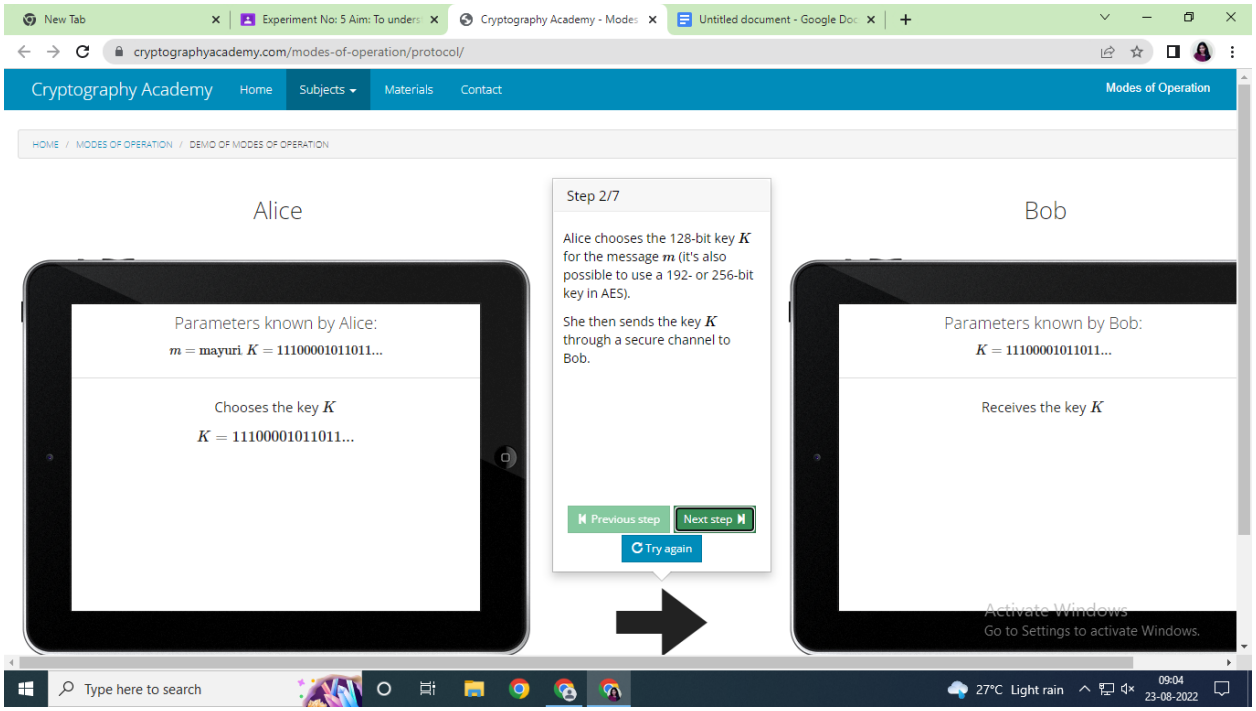

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 00010011101100...$, $p = 10$, $p_{16} = 00001010$,
$x = 01101101011000...$, $IV = 11101110000111...$,
$y = 11101110000111.....$
Encrypts the plaintext blocks x:
$z = E_K(IV)$
$= 00111010111110$
$y = x \oplus z$
$= 01010111100110...$
Typesetting math: 100%
Step 5/7
Alice first chooses the random 128-bits initialization vector \(IV \).
She then uses the key \(K \), the initialization vector \(IV \) and the AES encryption function \(E_{K} \) to encrypt the block \(x \).
Finally she sends the ciphertext block \(y \) to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 00010011101100...$, $IV = 11101110000111...$,
$y = 11101110000111.....$
Receives the ciphertext blocks y
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:04
23-08-2022

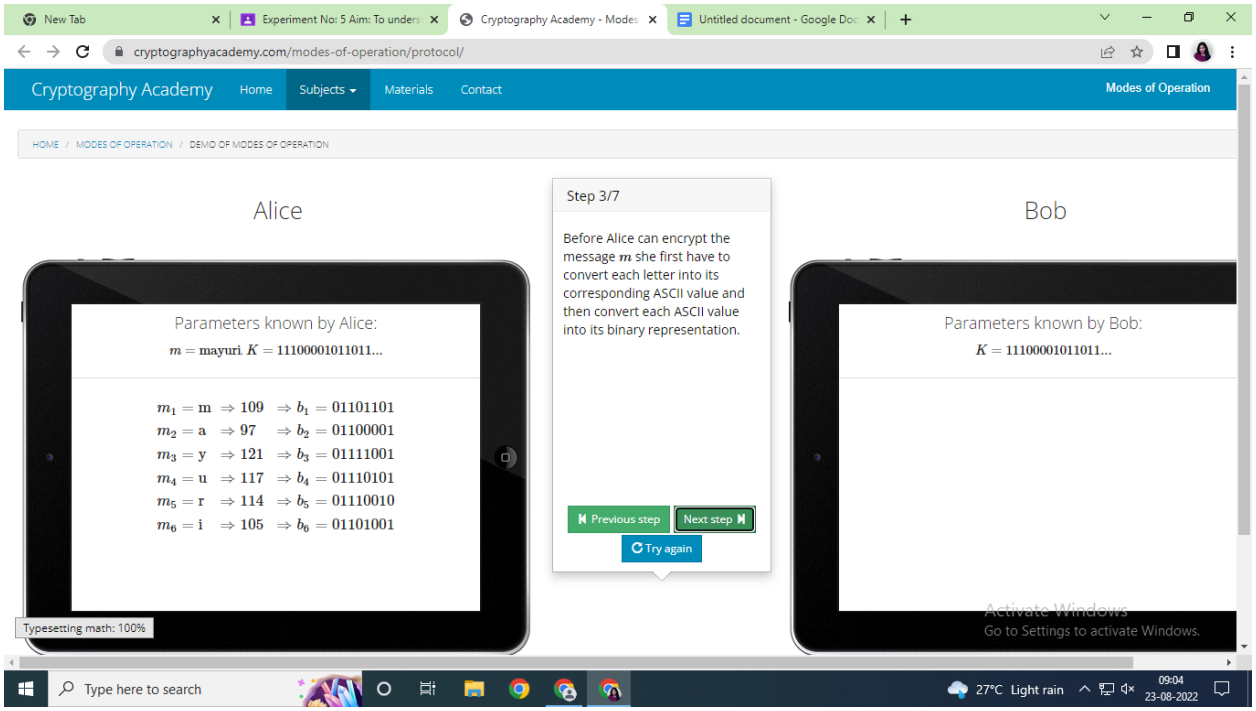

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 00010011101100...$, $p = 10$, $p_{16} = 00001010$,
$x = 01101101011000...$, $IV = 11101110000111...$,
$y = 11101110000111.....$
Typesetting math: 100%
Step 6/7
Bob uses the key \(K \), the initialization vector \(IV \) and the AES encryption function \(E_{K} \) to decrypt the block \(y \).
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 00010011101100...$, $IV = 11101110000111...$,
$y = 11101110000111.....$, $x = 01101101011000...$
Decrypts the ciphertext blocks y:
$z = E_K(IV)$
$= 01101101011000...$
$x = y \oplus z$
$= 01101101011000...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:04
23-08-2022

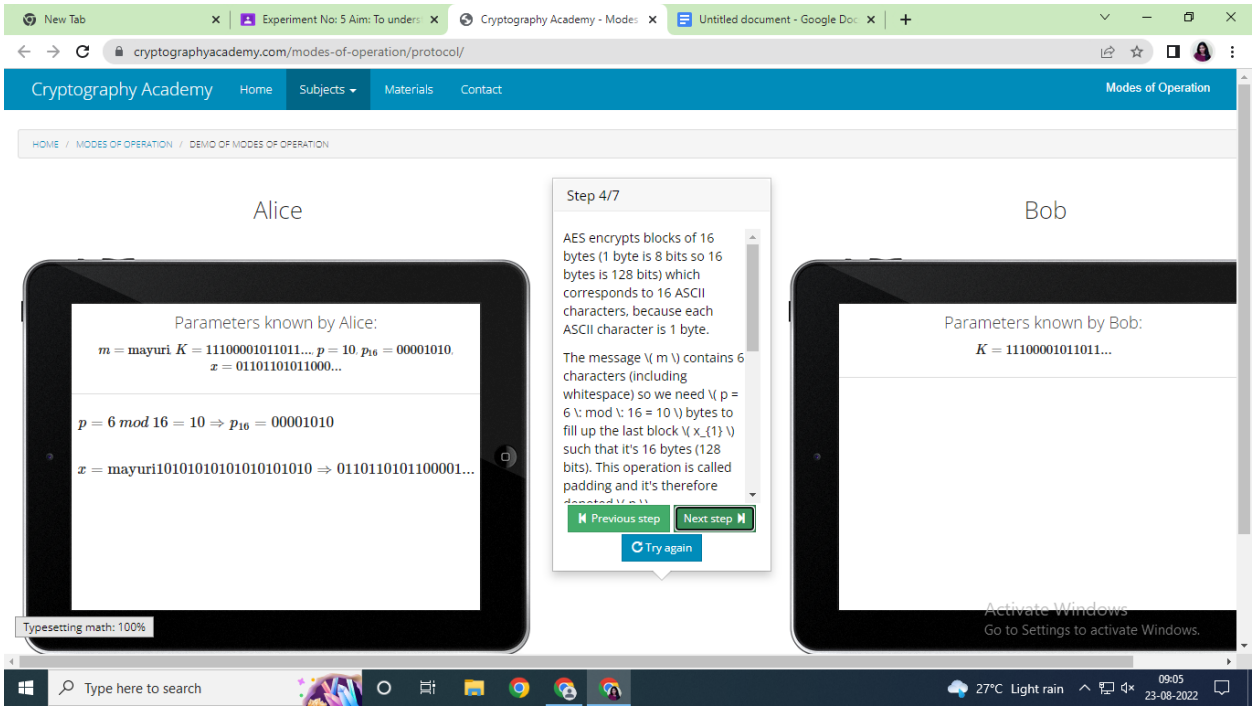

Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 7/7
Bob converts the first byte \(b_{1} = 01101101 \) in the block \(x \) to its integer representation \(109 \) and then to its letter representation \(m \).
Then he converts the rest of the bytes in the block \(x \).
Because the decimal value of the last byte \(p_{16} = 00001010\) in the last block \(x_{1} \) is \(p = 10\) and between 1 and 15, Bob know that the padding byte \(p_{16}
Previous step
Next step
Try again
Bob
Parameters known by Alice:
$m = \text{mayuri}$, $K = 00010011101100\ldots$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000\ldots$, $IV = 11101110000111\ldots$, $y = 11101110000111\ldots\ldots$
Parameters known by Bob:
$K = 00010011101100\ldots$, $IV = 11101110000111\ldots$, $y = 11101110000111\ldots\ldots$, $x = 01101101011000\ldots$, $p_{16} = 00001010$, $p = 10$, $m = \text{mayuri}$
$p_{16} = 00001010 \Rightarrow p = 10$
$x = 0110110101100001\ldots \Rightarrow \text{mayuri}10101010101010101010$
$m = \text{mayuri}$
Typesetting math: 100%
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:04
23-08-2022

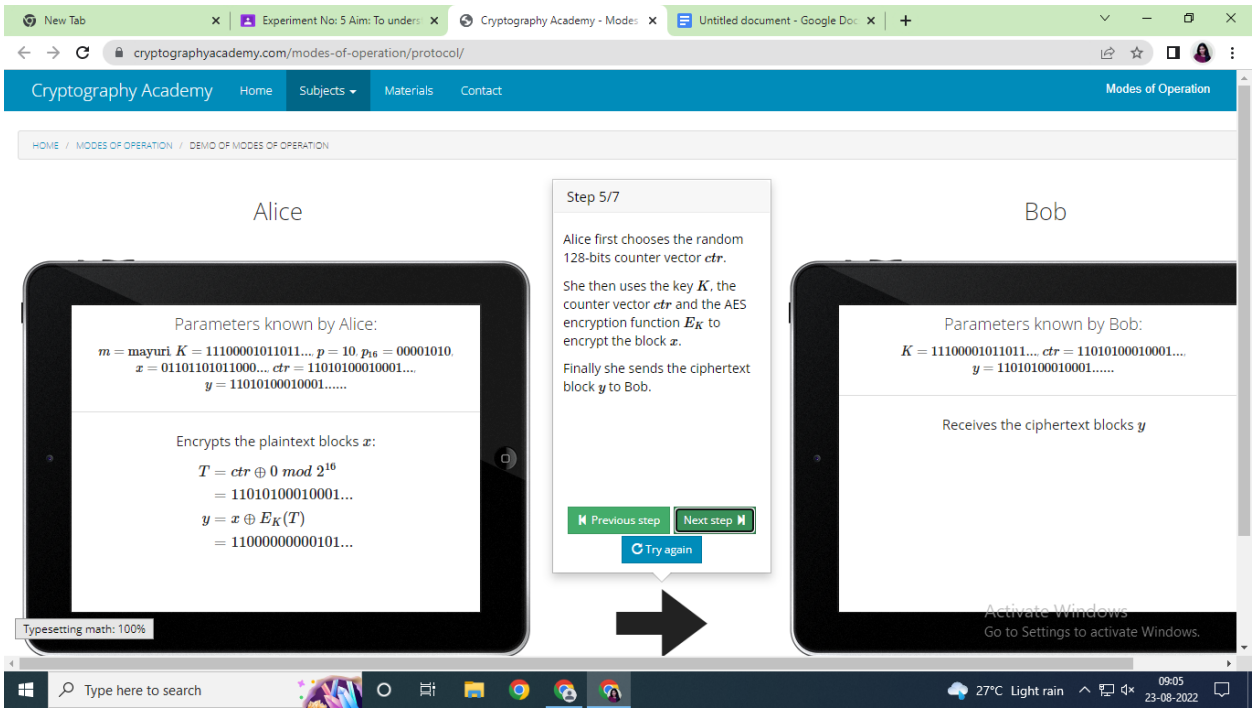
5) AES - CTR

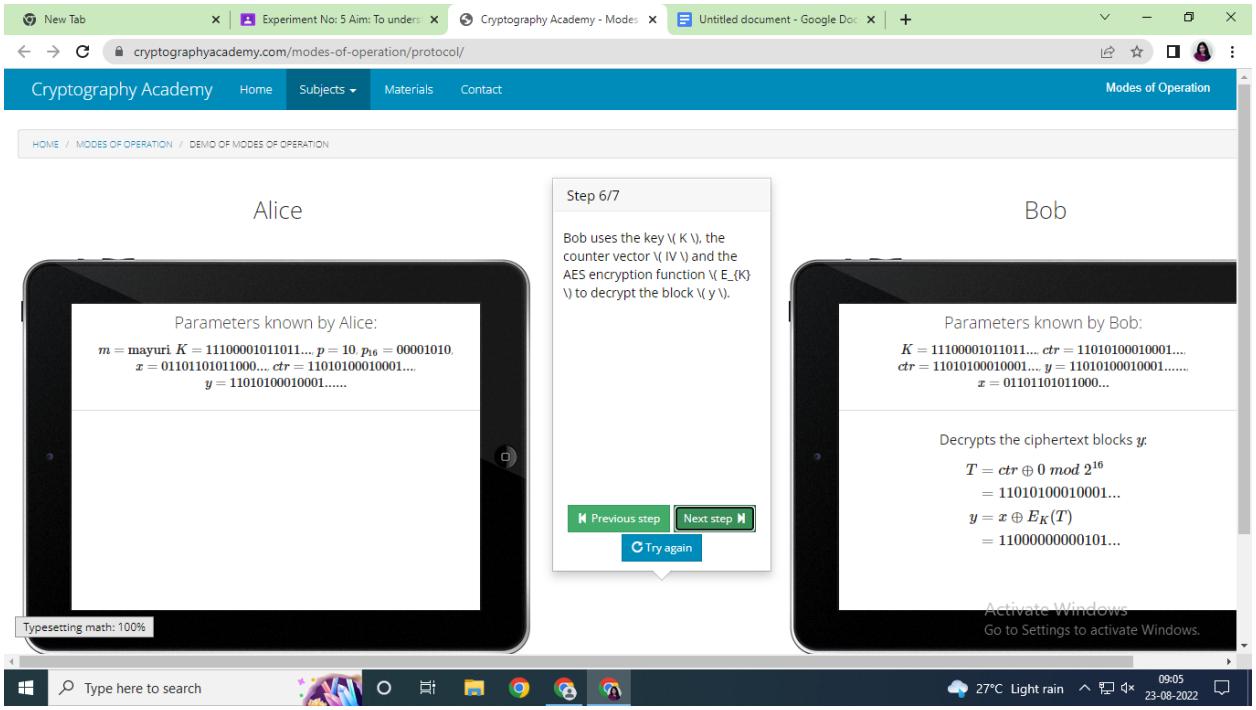

Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Step 1/7
Enter the message (or integer) that Alice wants to send encrypted to Bob:
mayuri
Use the following cryptosystem:
The Advanced Encryption Sta
With the following mode of operation:
Counter (CTR) mode
Previous step
Next step
Try again
Bob
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:04
23-08-2022

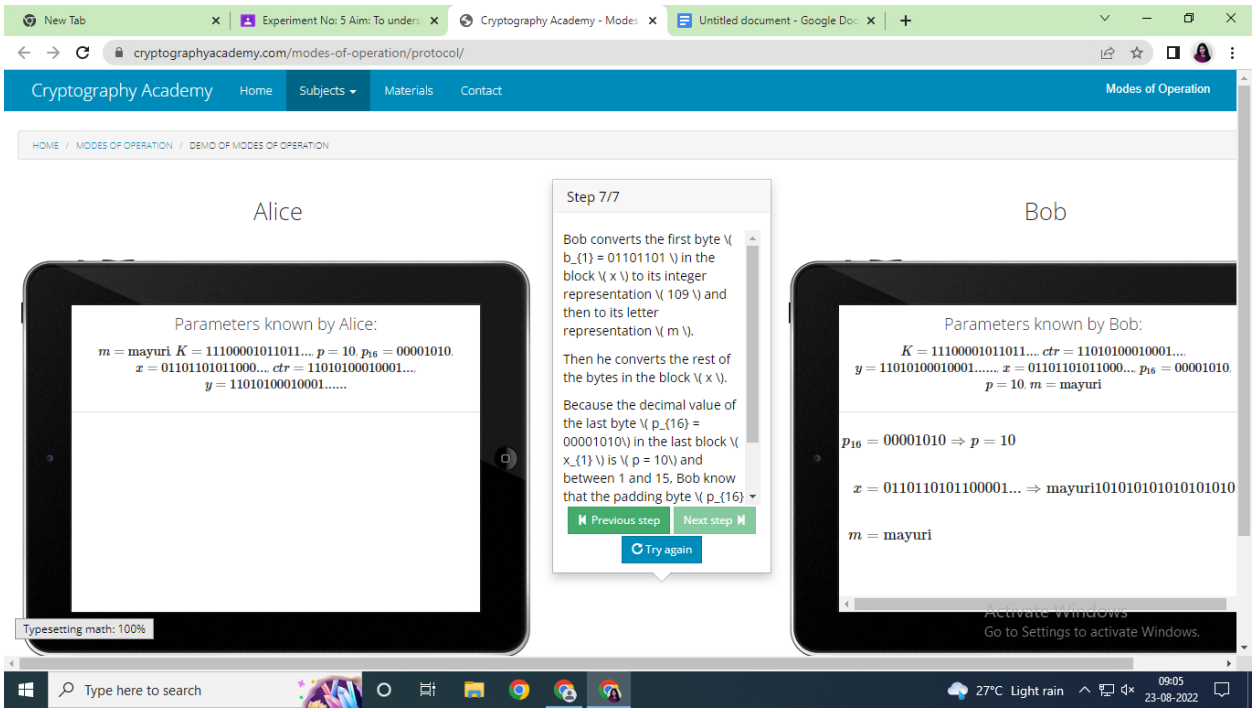

New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 11100001011011...$
Chooses the key K
$K = 11100001011011...$
Step 2/7
Alice chooses the 128-bit key K for the message m (it's also possible to use a 192- or 256-bit key in AES).
She then sends the key K through a secure channel to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11100001011011...$
Receives the key K
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:04
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$ $K = 11100001011011...$
$m_1 = \text{m} \Rightarrow 109 \Rightarrow b_1 = 01101101$
$m_2 = \text{a} \Rightarrow 97 \Rightarrow b_2 = 01100001$
$m_3 = \text{y} \Rightarrow 121 \Rightarrow b_3 = 01111001$
$m_4 = \text{u} \Rightarrow 117 \Rightarrow b_4 = 01110101$
$m_5 = \text{r} \Rightarrow 114 \Rightarrow b_5 = 01110010$
$m_6 = \text{i} \Rightarrow 105 \Rightarrow b_6 = 01101001$
Typesetting math: 100%
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11100001011011...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:04
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 11100001011011...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$
$p = 6 \ mod \ 16 = 10 \Rightarrow p_{16} = 00001010$
$x = \text{mayuri}1010101010101010101010 \Rightarrow 01101101011000001...$
Typesetting math: 100%
Step 4/7
AES encrypts blocks of 16 bytes (1 byte is 8 bits so 16 bytes is 128 bits) which corresponds to 16 ASCII characters, because each ASCII character is 1 byte.
The message \(m \) contains 6 characters (including whitespace) so we need \(p = 6 \: mod \: 16 = 10 \) bytes to fill up the last block \(x_{1} \) such that it's 16 bytes (128 bits). This operation is called padding and it's therefore
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11100001011011...$
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:05
23-08-2022


New Tab
Experiment No: 5 Aim: To unders
Cryptography Academy - Modes
Untitled document - Google Doc
cryptographyacademy.com/modes-of-operation/protocol/
Cryptography Academy
Home
Subjects
Materials
Contact
Modes of Operation
HOME / MODES OF OPERATION / DEMO OF MODES OF OPERATION
Alice
Parameters known by Alice:
$m = \text{mayuri}$, $K = 11100001011011...$, $p = 10$, $p_{16} = 00001010$, $x = 01101101011000...$, $ctr = 11010100010001...$, $y = 11010100010001.....$
Encrypts the plaintext blocks x:
$T = ctr \oplus 0 \ mod \ 2^{16}$
$= 11010100010001...$
$y = x \oplus E_K(T)$
$= 11000000000101...$
Typesetting math: 100%
Step 5/7
Alice first chooses the random 128-bits counter vector ctr.
She then uses the key K, the counter vector ctr and the AES encryption function E_K to encrypt the block x.
Finally she sends the ciphertext block y to Bob.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 11100001011011...$, $ctr = 11010100010001...$, $y = 11010100010001.....$
Receives the ciphertext blocks y
Activate Windows
Go to Settings to activate Windows.
Type here to search
27°C Light rain
09:05
23-08-2022





CONCLUSION: We successfully performed Encryption of long messages using various modes of operation using AES or DES.