## **Applied Cryptography Unit 1**

118 음



## You finished 26<sup>th</sup> Well done, keerthan pv!

Correct answers: 19/27 Voting time: 5:53

1	monisha	22/27	5:33
2	HarshithJ	22/27	6:37
3	Harsha Kanthraj	22/27	7:01
4	Anirudh Sripada Koundinya M	21/27	5:15
5	Mansha Taori	21/27	5:34

## Hide answers

## Which security goal is NOT directly addressed by cryptography?

1/27

Authentication

The total of all possible key combinations is known as the:

2/27

≪ Keyspace

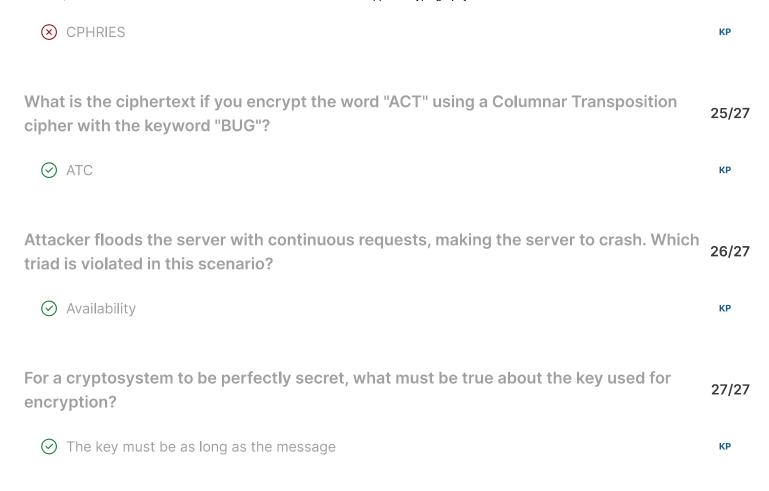
KP

The Playfair cipher uses what size of matrix for its key?	3/27
	KP
One-time pad requires:	4/27
■ Using the same key multiple times	KP
What is the major drawback of perfect secrecy systems like the One-Time Pad?	5/27
Key distribution and management	
The principle that prevents a sender from denying they sent a message is called:	6/27
○ Non-repudiation	KP
A "passive" attack on a system is one that:	7/27
Attempts to learn or make use of information	KP
What is an attack that tries every possible key called?	8/27
⊗ Brute-force attack	KP
In a brute-force attack, what percentage of keys must be tried on average to succeed?	9/27
	КР

The Vigenère cipher is an example of what type of cipher?	10/27
O Polyalphabetic substitution cipher	KP
Rail Fence Cipher is a type of:	11/27
	КР
A cipher that works by rearranging symbols, not replacing them, is a:	12/27
	КР
What is the primary difference between a "Known Plaintext" and a "Chosen Plaintext" attack?	13/27
	КР
Perfect secrecy means:	14/27
Using Caesar cipher, what is the ciphertext for the letter 'C' (P=2) with a key of 5?	15/27
	KP
How would the plaintext "BALLOON" be correctly converted into digrams for the Playfair cipher according to the rules shown?	16/27
Applied Cryptography Unit 1 MCQs	K
Applied Cryptography Unit 1 MCQs	К

a Caesar cipher?

The keyspace is much larger, making it more resistant to brute-force attacks.	КР
In the intercepted message "EQZP", which was decrypted by trying all possible Caesar shifts, "SEND" was found at shift 12. What does this process demonstrate?	18/27
A brute-force attack on a small keyspace	КР
In the Vigenère cipher example for "CYBERSECURITY", the key is "BEST". How is the key applied to the full plaintext?	19/27
	KP
Using the Caesar cipher, if you intercept the message "EHJL" and know it was encrypted with a shift key of 3, what is the plaintext?	20/27
	KP
What is 7 + 11 in Z15?	21/27
What is 7 + 11 in Z15?	21/27 кр
	•
<ul> <li></li></ul>	КР
<ul> <li></li></ul>	кр
<ul> <li></li></ul>	КР 22/27 КР
<ul> <li></li></ul>	кр 22/27 кр 23/27



Make your own Slido in minutes

slido