Applied Cryptography Unit 1

118

You finished 26th

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

✗ 4×4 KP

✓ 5×5

One-time pad requires: 4/27

✓ Key equal to message length

✗ 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

✓ 50%

✗ 80% KP

The Vigenère cipher is an example of what type of cipher? 10/27

✓ Polyalphabetic substitution cipher KP

Rail Fence Cipher is a type of: 11/27

✓ Transposition cipher KP

A cipher that works by rearranging symbols, not replacing them, is a: 12/27

✓ Transposition cipher KP

What is the primary difference between a "Known Plaintext" and a "Chosen Plaintext" attack? 13/27

✓ The cryptanalyst selects plaintext to be encrypted. KP

Perfect secrecy means: 14/27

✓ P[M=m|C=c]=P[M=m] for all m,c

Using Caesar cipher, what is the ciphertext for the letter 'C' (P=2) with a key of 5? 15/27

✓ H (P=7) 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

✓ BA-LX-LO-ON

What is the main advantage of a simple substitution cipher with a random mapping over a Caesar cipher? 17/27

✓ The keyspace is much larger, making it more resistant to brute-force attacks. KP

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 KP

In the Vigenère cipher example for "CYBERSECURITY", the key is "BEST". How is the key applied to the full plaintext? 19/27

✓ It is repeated until it matches the length of the plaintext. 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

✓ BEGI KP

What is 7 + 11 in Z15? 21/27

✓ 3 KP

An attacker uses letter frequency analysis on a simple substitution ciphertext, knowing the message was written in English. What is this type of cryptanalytic attack called? 22/27

✓ This is a cryptanalytic attack relying on plaintext characteristics. KP

In the Hill cipher, what is the correct formula for Encryption scheme? 23/27

✓ C=M . P mod 26 KP

If the plaintext "CIPHERS" is encrypted using a Rail Fence cipher with 3 rails, what is the resulting ciphertext? 24/27

✓ CESIPRH

✗ CPHRIES KP

What is the ciphertext if you encrypt the word "ACT" using a Columnar Transposition cipher with the keyword "BUG"? 25/27

✓ ATC KP

Attacker floods the server with continuous requests, making the server to crash. Which triad is violated in this scenario? 26/27

✓ Availability KP

For a cryptosystem to be perfectly secret, what must be true about the key used for encryption? 27/27

✓ The key must be as long as the message KP