Cryptography Questions 2

Table of contents

Anish Goyal Schepens Period 1 01/30/2023

What is most significant difference between Symmetric Key Encryption and Asymmetric Key Encryption?

Symmetric key encryption uses the same key to encrypt and decrypt the message. Asymmetric key encryption uses two keys, one to encrypt and one to decrypt the message.

What method is used to exchange safe keys between two parties that are in two different locations?

Diffie-Hellman Key Exchange is the method that is used to exchange safe keys between two parties that are in two different locations.

What is the function of a Certificate Authority?

The function of a Certificate Authority is to validate identities on the Internet by issuing digital certificates containing cryptographic keypairs.

Who are some of the most widely used Certificate Authorities?

Some of the most widely used Certificate Authorities are Entrust, Verisign, GlobalSign, DigiCert, Comodo, and GoDaddy

What is the primary use of a Digital Certificate?

The primary use of a Digital Certificate is to verify the identity of a website or organization.

What was the Enigma Machine? How did it work?

The Enigma Machine was a permutation cipher used by the Nazis to encrypt and decrypt messages in World War II. It worked by using a series of wheels known as Enigma rotors that would scramble the message. The rotor could swap the order of the letters and rotate the rotors such that the ciphertext would have many different possible outputs. Both the sender and receiver would have to know the order of the rotors and the starting position of the rotors in order to decrypt the message.

Which organization cracked the Enigma Code? How did they do this?

The French secret service, Polish Cipher Bureau, and British cryptological establishment were organizations that contributed to cracking the Enigma Code. They did this by using a machine called the Bombe, which was a mechanical device that could decrypt the Enigma Code, and brute forcing rotor combinations that satisfied the constraints of messages that would always contain "Weather" and "Heil Hitler" in it.

What are 3 significant facts of the person most responsible for cracking the Enigma Code?

Alan Turing was the person most responsible for cracking the Enigma Code. Three significant facts about him are: 1. Alan invented the Turing Machine, which was a model that manipulated symbols on a tape according to a tableset of rules. It was capable of implementing any computing algorithm. 2. Turing was prosecuted for homosexuality and was forced to undergo chemical castration by the British government. In 2017, the United Kingdom passed "Turing's Law," which posthumously pardoned homosexuals who were convicted under the law. 3. Turing created the Turing Test, which requires a computer to be able to pass as a human in a text-based conversation in order to be considered intelligent. The Turing Test is used to diagnose whether a computer is intelligent or not in today's world.