Cryptography Questions 1

Table of contents

Anish Goyal Schepens Period 1 01/27/2023

Explain what Defense in Depth means

Defense in depth is a security strategy that is used to make sure that if one part of the security fails, there is another part of the security that will still protect the system. It is a way to make sure that the system is protected even if one part of the security fails. For example, if a firewall is breached, there is another layer of security like an IDS/IPS or a VPN that will still protect the system.

What are the three "parts" of the Enigma machine and how did what did they do to encrypt text?

The three parts of the Enigma machine are the rotors, the reflector, and the plugboard. The rotors are the part of the machine that actually encrypted the text. The reflector is the part of the machine that reflected the encrypted text back to the rotors. The plugboard was the part of the machine that connected the wires to the rotors (mapping the letters from the rotors to the letters on the plugboard through wires).

What did the enigma do with each key stroke that made it even harder to crack?

The enigma machine would rotate the rotors every time a key was pressed. This made it even harder to crack because the rotors would be in a different position every time.

What is DES and AES? What did AES do that DES did not?

DES is the Data Encryption Standard. It is a symmetric encryption method that uses a key to encrypt and decrypt data. AES is the Advanced Encryption Standard. It is also a symmetric encryption method that uses a key to encrypt and decrypt data. AES is more secure than DES because it uses a 256-bit key instead of a 56-bit key. In In AES the entire data block is processed as a single matrix, while in DES, the data block is divided into 64-bit sub-blocks and each sub-block is processed as a separate matrix.

How many keys did DES support?

56

What is the math used behind the Diffie Hellman Key Exchange?

Uses modular exponentiation - $(a^x)^m \mod n$ - a is the base - x is the exponent (the public key of the receiver) - n is the modulo, which is a prime number agreed on the client and server - m is the private key of each party - Works because the receiver can't figure out the private key of the sender, but once it sends its public key, the original message is intact because of exponent multiplication rules

What is the part of the math equation that is difficult for hackers to figure out? This makes it hard to crack.

It is extremely difficult to calculate/brute force the exponent m given the base, modulo, and the public key given numbers containing more than 100 digits. The private keys are also regenerated every time a new session is started, making it even harder to crack.

What are the differences between how Asymmetric and Symmetric Encryption methods work?

Symmetric encryption uses a private key to encrypt and decrypt an encrypted email while asymmetric encryption uses the public key of the recipient to encrypt the message.

How does the Vigenère Cipher work? How is it different than the Caesar Cipher?

Vigenère Cipher is a polyalphabetic substitution cipher. It uses a series of Caesar Ciphers with different keys. On the other hand, the Caesar Cipher is a monoalphabetic substitution cipher. It uses a single shift to encrypt and decrypt the message.