جامعة الأمير سطام بن عبدالعزيز
PRINCE SATTAM BIN ABDULAZIZ UNIVERSITY

Homework 2
Cryptography

Name:
Manar Al-Munyif
441960354

Q.1 Compare and contrast cryptographic Algorithms used in following:
-Banking Applications
-Online Shopping Applications

1-Banking Applications:

In today's online world, the risk of unauthorized access to all types of data is always present. Most vulnerable is financial and payment system data, which can expose customers and customers' personally identifiable information (PII) or payment card details. Encryption is critical to protecting personal data and reducing the risks faced by companies conducting payment transactions every day.

Symmetric encryption:

It is an encryption method that uses only one key (secret key) to encrypt and decrypt electronic data. Entities communicating via symmetric encryption must exchange a key so that it can be used in the decryption process. This method of encryption differs from asymmetric encryption in that it uses a pair of keys (a public key and a private key) to encrypt and decrypt messages.

Using a symmetric encryption algorithm, the data is & quot ; scrambled &quot ; so that it cannot be understood by anyone who does not have the key to decrypt it. Once the intended recipient who owns the key has the message, the algorithm reverses its work so that the message is returned to its original readable form. The secret key used by both the sender and recipient can be a certain password/code or it can be a random string of letters or numbers generated by a secure random number generator (RNG). For bank-grade encryption, symmetric keys must be generated using an RNG that has been certified by industry standards, such as FIPS 140-2.

There are two types of symmetric encryption algorithms:

1. Blocking algorithms. Lengths of bits are encrypted into blocks of electronic data using a specific secret key. While encrypting data, the system keeps the data in its memory while it waits for complete blocks.
2. Streaming algorithms. Data is encrypted as it flows rather than being kept in system memory.

Some examples of symmetric encryption algorithms include:

* AES (Advanced Encryption Standard)
* Data Encryption Standard (DES)
* IDEA (International Data Encryption Algorithm)
* Blowfish (immediate replacement for DES or IDEA)
* RC4 (Rivest Cipher 4)

* RC5 (Rivest Cipher 5)
* RC6 (Rivest Cipher 6)

AES, DES, IDEA, Blowfish, RC5, and RC6 are block ciphers. RC4 is the encoder stream.

DES

In "modern" computing, DES was the first cipher standard to secure electronic communications, and is used in various forms (such as 2-key or 3-key 3DES). The original DES is no longer used because it is considered too "weak", due to the processing power of modern computers. Even 3DES is not recommended by NIST and PCI DSS 3.2, and so are all 64-bit zeros. However, 3DES is still widely used in EMV chip cards due to older applications that do not have an EMV file.

AES

The most widely used symmetric algorithm is Advanced Encryption Standard (AES), which was originally known as Rijndael. This is a standard developed by the US National Institute of Standards and Technology in 2001 for the encryption of electronic data announced in US FIPS PUB 197. This standard replaces DES, which has been in use since 1977. Under NIST, AES encryption has a block size of 128 bits, but It can have three different key lengths as defined in AES-128, AES-192, and AES-256.

What is the use of symmetric encryption?

While symmetric encryption is an older method of encryption, it is faster and more efficient than asymmetric encryption, which negatively impacts networks due to performance issues related to data size and CPU intensive usage. Due to the better performance and faster speed of symmetric encryption (compared to asymmetric encryption), symmetric encryption is usually used to encrypt/encrypt large amounts of data, for example to encrypt a database. In the case of a database, the secret key may only be available to the database itself to encrypt or decrypt. Standard symmetric encryption is also less vulnerable to quantum computing advances than current standards for asymmetric algorithms (at the time of writing).

Some examples of the use of symmetric encryption are:

* Payment applications, such as card transactions where protection of PII is required to prevent identity theft or fraudulent charges
* Validations to confirm that the sender of the message is who it claims to be
* Generate random numbers or hashes

2-Online Shopping Applications:

Technological advancements have made online shopping an interesting thing, providing online access and payment for products or services. However, security remains a concern. Sniffers, phishing, and other social engineering techniques often prevail against existing security systems. Therefore, this research proposes a framework that actively engages customers in their online shopping and payment processes using the Online Payment Alternative Solution (OPAS), a mobile application developed. To enhance the security of the proposed framework, a one-time dynamic password (OTP) blowfish cipher and a one-time password encryption key (OTPEK) generation algorithm are used. The One Time Password (OTP) and encrypted OTPEK are then included as a captcha using Least Important Information Steganography (LSB); It is then sent to the customer's OPAS for payment approval in near real time. The systems developed have been tested and found to work accurately based on the test cases generated.

Encryption is the process of hiding the meaning of data so that only specified parties can understand the contents of the transmission (Shoretel, nd). It plays a very important role while shopping online. Secure electronic commerce is made possible by a type of encryption known as public key cryptography. This method relies on two keys that are mathematically related, but different: a public key and a private key (Proffitt, 2013). Public key cryptography is an asymmetric key algorithm, which means that the key used to encrypt the message does not have the ability to decrypt it either. The public key is used to encrypt messages, while the private key is used to decrypt messages. In contrast, symmetric key algorithms use a single key that encrypts and decrypts messages.

The level of security of public key cryptography depends on the randomness of the keys used. The keys must be large prime numbers and must be randomly generated to ensure that no machine can efficiently deduce the identity of the keys (Proffitt, 2013). Public keys are shared freely, while private keys are kept private. In order to send an encrypted message to a particular party, all one has to do is encrypt the message with the intended recipient's public key, and send it. An encrypted message can only be decrypted with the recipient's private key; Thus, only that person can decrypt them, since only he or she possesses the required private key. It is impossible to deduce an individual's private key from the public key in a reasonable amount of time, which explains why public keys are public knowledge. on the other side.

How does encryption keep your personal information private?

Encryption enables e-commerce. Transport Layer Security (TLS) is the most common encryption protocol used to ensure security during an e-commerce transaction (Proffitt, 2013). Secure Sockets Layer (SSL) is an older but also popular encryption protocol (Proffitt, 2013). Through a combination of asymmetric and symmetric key encryption, TLS is able to create a significant level of security for consumers across the Internet.

The benefits of encryption

Without encryption, e-commerce would not be sustainable. Every online transaction carries a risk of financial or identity theft, and if credit card information is not encrypted, it could fall into the hands of a fraudulent third party (Shoretel, n.d.). Encryption protects data by preventing unwanted people from reading information. Without encryption, if a hacker intercepts the communication between your browser and the retailer's web server, they can easily read your sensitive data. How would you feel if your credit card information was stolen? Are you crazy? harm? Endangered? Therefore, the importance of encryption cannot be overemphasized. In the collective world where online shopping is common, the confidentiality of your information depends on encryption. As long as the encryption is in place, you don't have to worry about the security of online shopping all the tim.

References:

[1] Al- Amin, Ammar Muhammad Abdullah 2016, Improving the DES encryption algorithm using multiple keys

[2] Rahma, Ali Muhammad Dahab 2013, Cryptography and Information Security

[3] Abdel- Rahman Wajdi Essam 2007, Introduction to encryption by classical methods [18] Tohme, Hassan, Yassin, Analysis and design of algorithms

[4] Mostafa Sadeq International Blog, 2014, encryption and its types