TUTORIALS 7253

CRYPTOGRAPHY: HOW IT HELPS IN OUR DIGITAL WORLD

By: Zia A. Sardar

Abstract:

This application note is part of a series that is designed to provide a quick study guide in cryptography for a product development engineer. Each segment takes an engineering rather than theoretical approach on the topic. Gain an understanding of the basic concepts of cryptography, along with tips to quickly integrate security into your design. A similar version of this application note originally appeared on April 2, 2020 on Electronic Design.

Why Is Cryptography Needed?

Cryptography is used everywhere in our daily lives. Each time you make an online purchase, conduct a banking transaction, or ping your email client, cryptography is working in the background. It secures all transmitted information in our IoT world, to authenticate people and devices, and devices to other devices. Without cryptographic engines and functions, our modern world would come to a halt and all our important information would be exposed for potential exploitation.

Classical Cryptographic Techniques

Classically, cryptography used **"security by obscurity"** as way to keep the transmitted information secure. In those cases, the technique used was kept secret from all but a few, hence the term **"obscurity."** This made the communication secure, but it was not very easy to implement on a wide scale. Classical cryptographic methods are only secure when two parties can communicate in a secure ecosystem.

Figure 1 displays a classical cryptographic system. The sender and the receiver first agree upon a set of pre-shared encryption/decryption keys. These keys are then used sequentially to encrypt and then de-crypt each subsequent message.

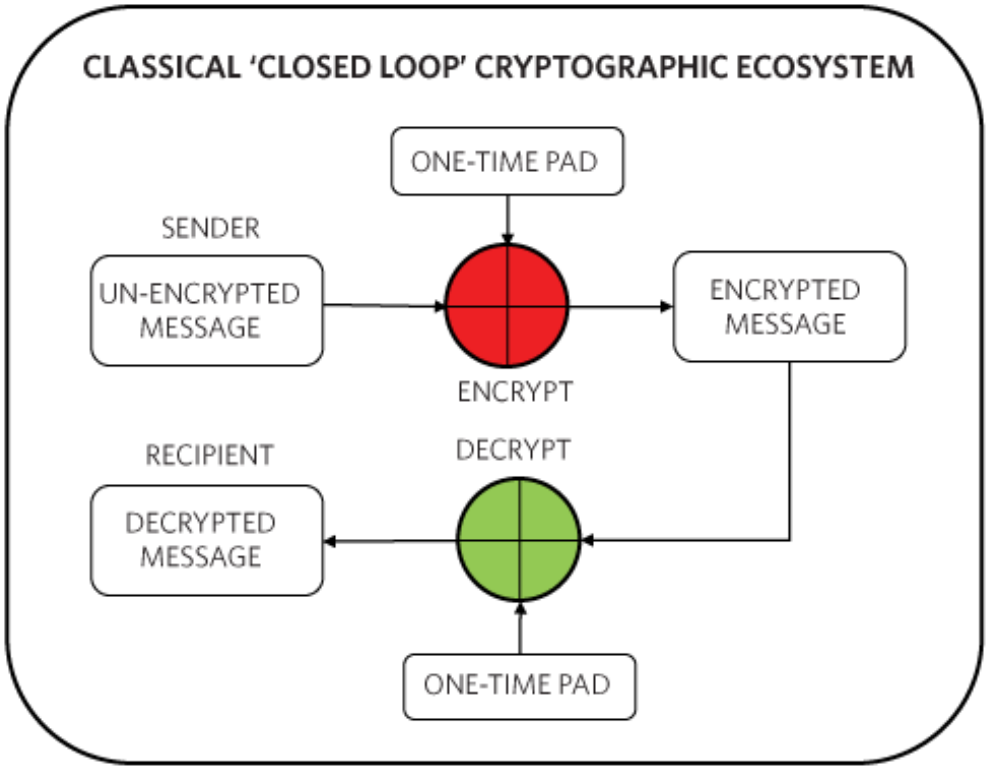

Figure 1. A classical closed-loop cryptographic system uses one-time pad as an encryption technique.

One-time pad is an encryption technique that requires the use of a one-time pre-shared key that is the same size or longer than the message being sent. This key must be the same one used for encryption.

The term **"One-Time Pad"** is an artifact from having each key on a page of a pad that was used and then destroyed. Once the pre-shared keys are exhausted, the sender and the receiver need to meet in a secure location to securely exchange a new set of keys and then store them in a secure location for the duration of the next set of message exchanges.

Clearly, obsolete classical techniques are no longer viable. Today, a vast system of electronic communication, commerce, and intellectual properties needs to be secured across oceans and continents that would otherwise be intercepted by people with hostile intentions.

Cryptography for the IoT Age

The IoT age demands an excellent level of security for a massive system that can carry out billions of transactions in a short period. That's where modern cryptography comes in. It is an essential part of **secure but accessible** communication that is critical for our everyday life.

Next, we will learn how this is achieved on a day-to-day basis all around us. We rely on publicly known algorithms for securing the massive amount of information that is exchanged around the clock. These algorithms are standards-based and vetted in an open environment so that any vulnerabilities can be quickly found and addressed.

Figure 2 shows a simplified modern cryptographic system. Let's investigate these systems and algorithms a bit more in depth.

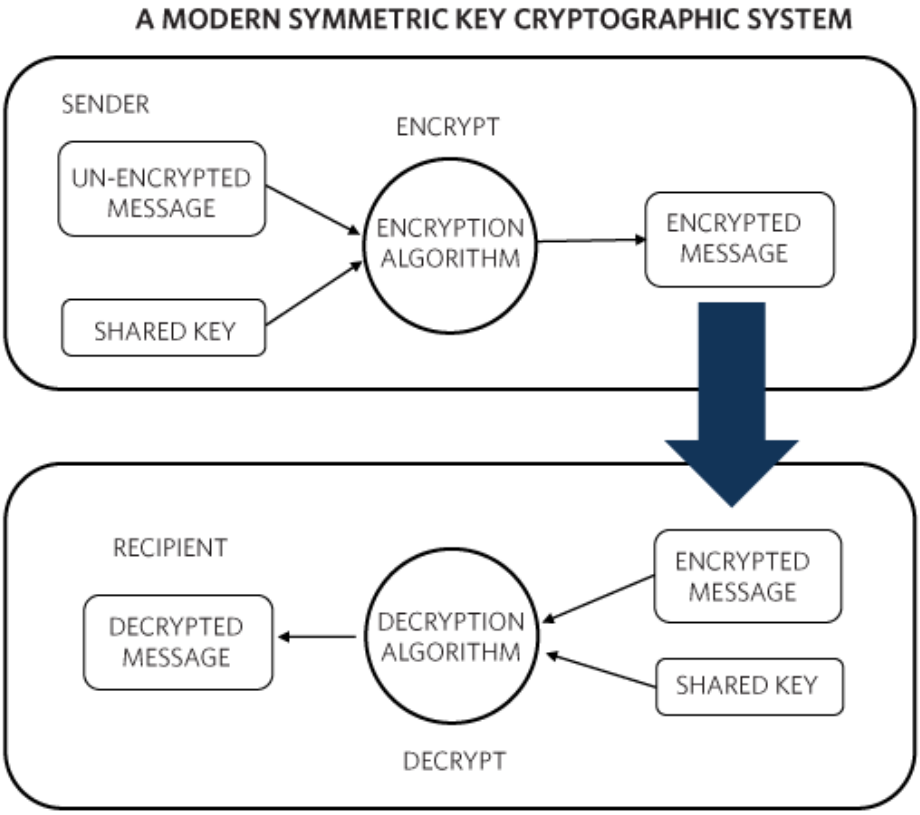

Figure 2. Modern symmetric key cryptographic system provides a greater level of security.

The basic tenant of a modern cryptographic system is that, instead of depending on the secrecy of the algorithm used, we rely on the secrecy of the keys. A modern cryptographic system has four main goals:

- **Confidentiality:** Information can never be disclosed to someone who is not authorized to see it.
- **Identification and Authentication:** Before any information is exchanged, identify and then authorize both the sender and the recipient.
- **Integrity:** Information must not be modified in storage or transit. Any modification must be detectable.
- **Non-repudiation:** Cannot disclaim the creation/transmission of the message. This provides "digital" legitimacy and traceability of a transaction.

Current cryptographic systems provide all the above or a combination of the above in various forms for an intended application. Let's explore each of these goals a little more to get a basic idea of how they are achieved.

Confidentiality

Confidentiality requires information to be secured from unauthorized access. This is accomplished by encrypting a sent message using a cryptographic algorithm with a key that is only known by the sender and recipient. An interceptor might be able to obtain an encrypted message but will not be able to decipher it.

Figure 3 shows how encryption is used. In this case, the sender and recipient have worked out a system to share the encryption/decryption key. They both use the key to encrypt/decrypt the messages they exchange between each other. If a malicious individual intercepts the message, no harm is done since that person will not have the key to decrypt the message.

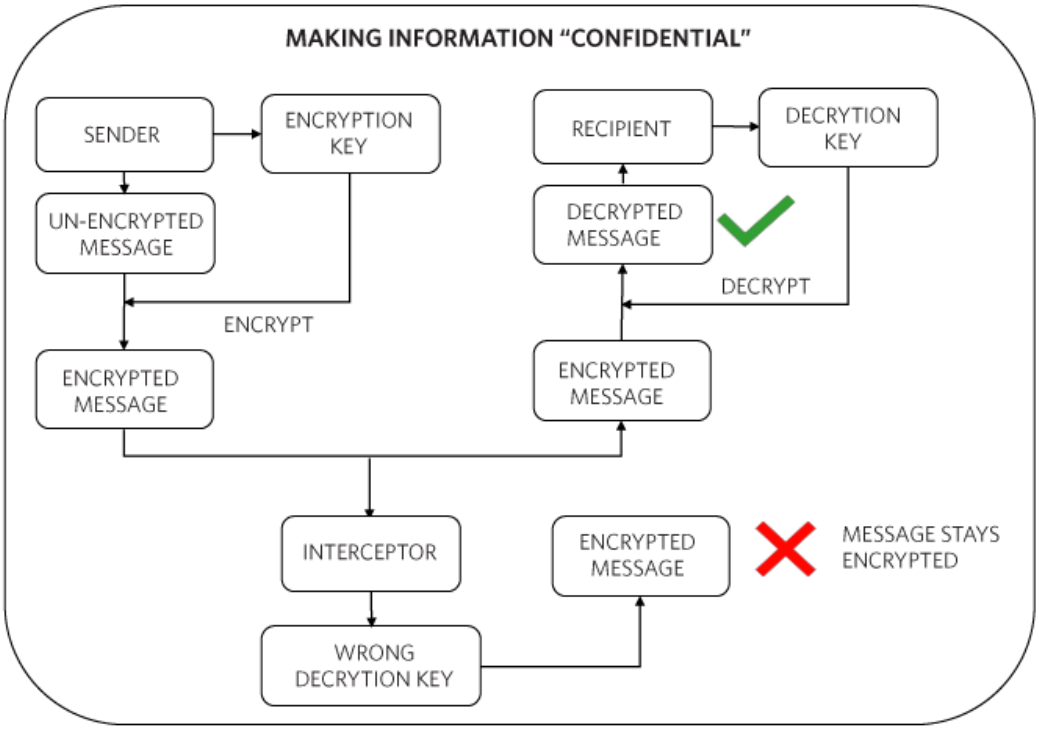

Figure 3. Encryption ensures information is kept confidential.

Identification and Authentication

The goal here is to first identify an object or a user and then authenticate them prior to initiating communication or other operations. Once the Sender has authenticated the Recipient, further communication can begin.

To learn more about the basics of authentication, please watch the video, "Security Short Subjects: Basics of Authentication."

In Figure 4, we show how authentication works in one direction. The bank (Sender) authenticates the customer's PC (Recipient) using a simple username and password combination before letting the customer use the bank's website. The actual process is much more complex, but we are using this

simple example to illustrate the basic concepts of cryptography. Identification and authentication can also be a bidirectional process, where the Sender and Recipient both need to identify each other before starting message exchanges.

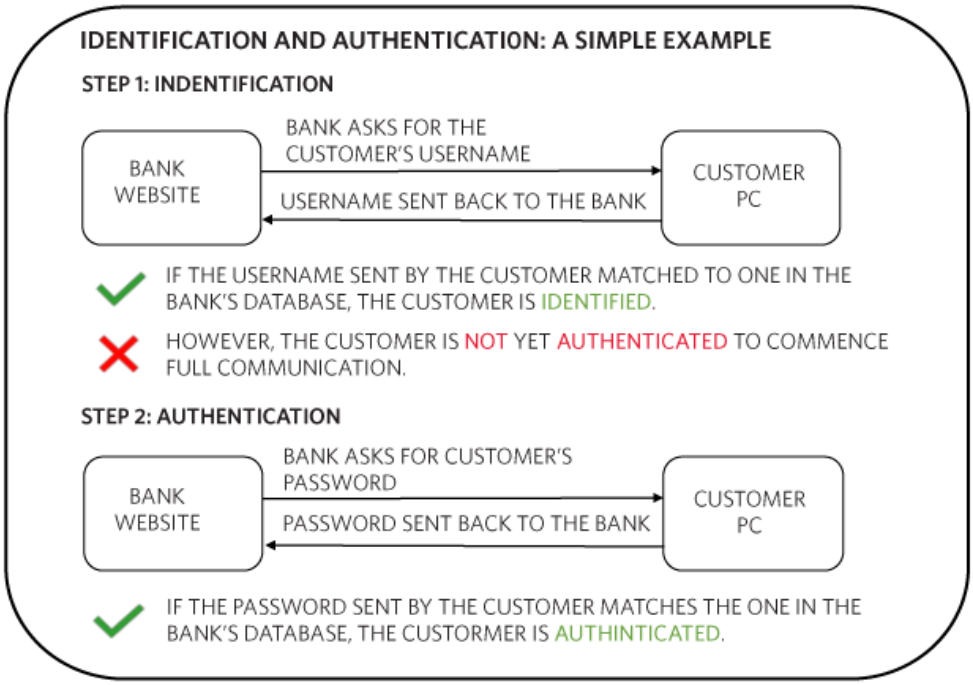

Figure 4. Identification and authentication, basic concepts of cryptography, work in one direction.

Integrity

How do we make sure that a message sent and then received over a communication network or data link hasn't been altered during transit? For example, there could be an attempt to intercept a message and insert a virus or malicious program to take control of the Recipient's PC or other equipment without their knowledge. To prevent this from happening, it is vital to ensure that any message transmitted is not modified.

As shown in **Figure 5**, one way to do this is to use a message digest. The Sender and Recipient use an agreed upon Message Digesting Algorithm to create and verify the match of the message digest output. If the message is altered, the message digests will not match and the Recipient knows that either tampering has occurred or there was a transmission error. There are many Message Digesting Algorithms that are used in modern cryptographic applications including SHA-2 and, most recently, SHA-3.

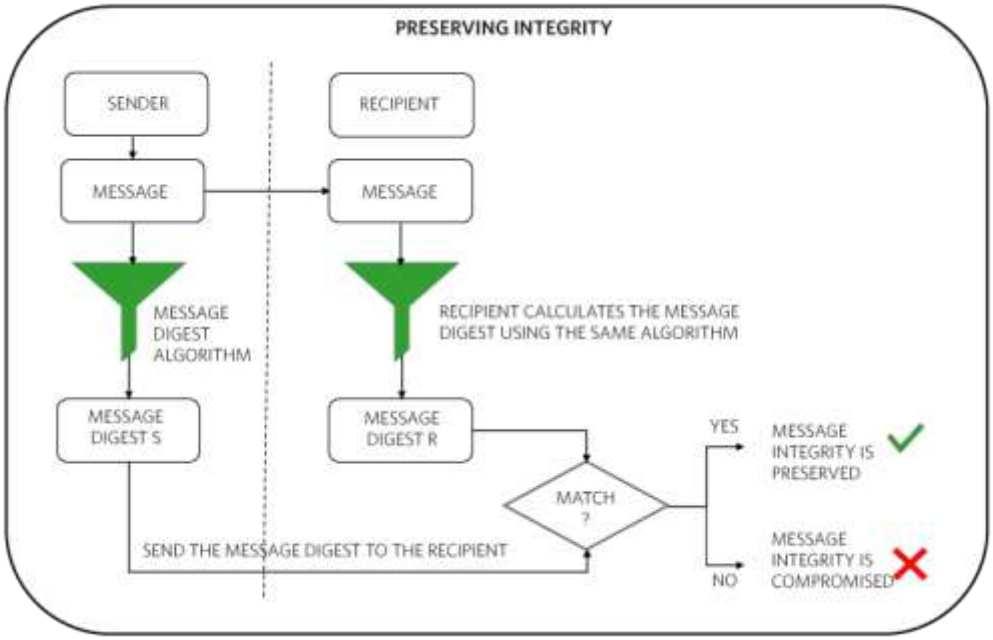

Figure 5. Using a message digest helps both a sender and recipient to preserve integrity.

Non-Repudiation

In a communication system where a multitude of messages are exchanged, there's a need to trace the incoming message back to the Sender. This is required to ensure that the Sender does not deny sending the message. Like a pen-and-paper legal document that we sign to finalize, a digital signature is used to achieve similar goals in the digital domain.

Figure 6 shows a simplified view of the digital signature generation, transmission, and verification process. First, the Sender takes the outgoing message and puts it through a Message Signing Algorithm to generate a digital signature related to the message and the Sender's verified identity. The Sender then attaches the digital signature to the original message and sends it to the Recipient. The Recipient takes the incoming combined message and separates the original message and the digital signature. Both are then input into a Message Verification Algorithm. The result can then be used by the Recipient to prove that the message was signed by the Sender.

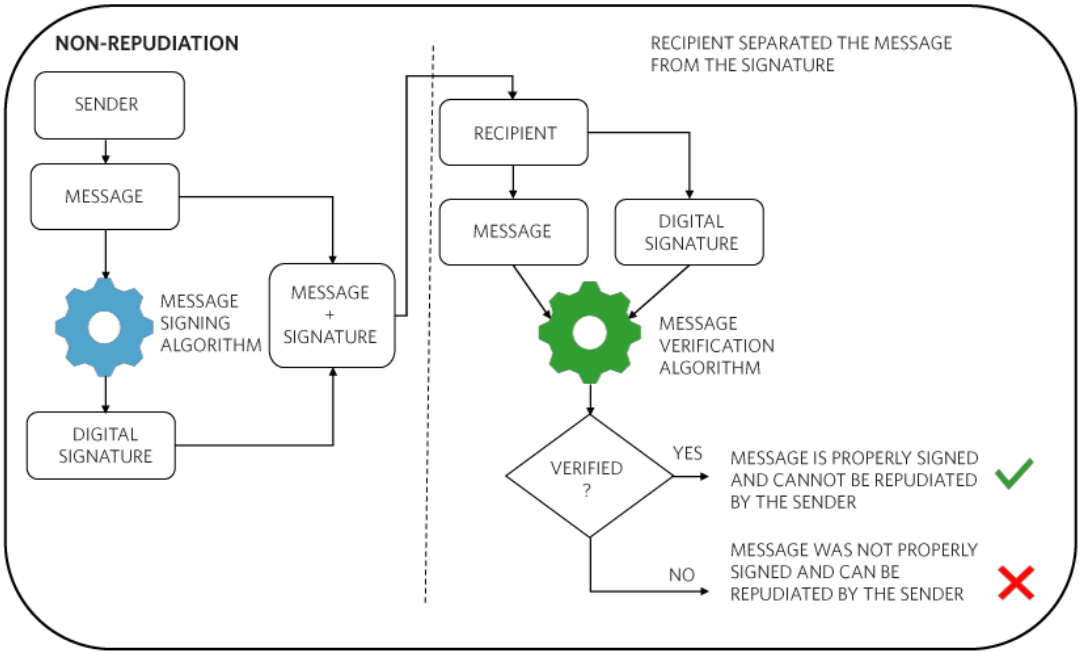

Figure 6. The non-repudiation process includes digital signature generation, transmission and verification.