FIPS 140 Demystified

An Introductory Guide for Developers

Wesley Hisao Higaki
Ray Potter

Excerpt for SafeLogic

Chapter 3: Encryption Is the Solution

The previous chapter highlighted the threats and risks to electronic information in today's highly-connected world. There are many computer and network security technologies available to consumers and enterprises including firewalls, anti-virus software, and intrusion detection systems. While all of these protection technologies serve their purpose, encryption is the foundational technology used to protect data. Encryption is the last line of defense.

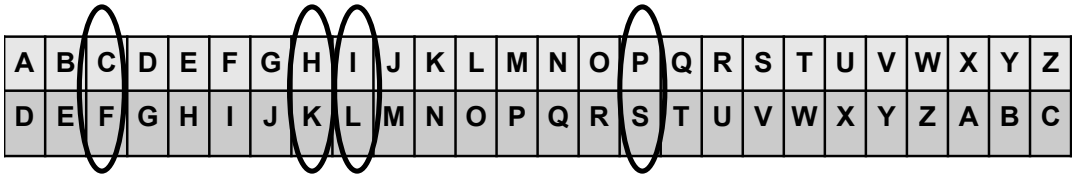
Encryption technologies have evolved in sophistication from the Caesar cipher which merely shifted character order in the alphabet to 256-bit symmetric keys used in today's Advanced Encryption Standard (AES). Encryption has always been a key data protection technology and has evolved with our security needs.

The Caesar Cipher

A cipher is a simple character substitution encoding scheme. A letter in the alphabet is replaced by another letter in the encoded message. Like the secret decoder ring that was popular in breakfast cereal boxes of the 1960's, the trick to decoding the messages was to know the shift in the alphabet that was used to encode the message.

For example, if the word "chip" were to be encoded using a three-letter offset cipher, the "c" in "chip" would appear as an "f" in the encoded message since "f" is three letters away from "c" in the alphabet. The "h" would be replaced by a "k"; the "i" with an "l"; and "p" would be represented by an "s". The word "chip" would be encoded using the three-letter offset as "fkls".

To illustrate the cipher, the English alphabet is lined up at the top of the diagram below. The three-letter shift cipher is shown below the alphabet. To code any word or message using this scheme the sender merely replaces the letter from the top row with the letter from the bottom row.



Julius Caesar used the cipher to encode messages to his troops during battle. This simple but clever mechanism allowed him to communicate securely in a hostile environment where secrecy was paramount.

It is estimated that the worldwide market for electronic information security software technologies in 2010 will be over 16.5 billion dollars [Gartner 2010]. These revenue figures include products such as firewalls, virtual private networks, intrusion detection systems and anti-virus. While these products protect data and information systems in different ways, they merely provide the "outer layers" of protection in the "defense in depth" schemes commonly used today. Encryption protects the data when the other defense mechanisms fail. When a hacker wriggles through an open port in a firewall and gains root access to a server, the intrusion detection system may report the intrusion but cannot actively protect the data. In ancient times a Roman messenger may have been captured while trying to relay a message from Caesar but the cipher made the message unreadable. Similarly, modern electronic data encryption renders the bits on the disk useless to the hacker even after he has broken through all of the other barriers.

E-commerce has permeated all facets of consumer and business life to the point that protecting data is critical to not only the continued success of commerce but to its very survival. If consumers and businesses lose confidence in the security of their online transactions, e-commerce will cease. With so much at stake it is imperative that key security technologies such as cryptography keep ahead of the threats and attacks and continue to instill customer confidence.

Encrypting Data in Transit

Electronic data is most vulnerable when it is being transmitted across open, public networks. A clear example of this vulnerability is "war driving" which is when attackers, intruders and pirates gain unauthorized access to unsecured wireless networks by merely driving by wireless access points using some fairly unsophisticated equipment. Gaining network access is just the first step toward collecting confidential data. Data transmitted over these wireless networks could be "sniffed" and exploited by malicious parties.

Installing a set of wireless access points in an office building can save thousands of dollars in network installation costs compared to running miles of the traditional Category 6 Ethernet cable through the facility. Unfortunately, installers may not be thorough and can fail to enable the secure communications features on the access point devices. When the access points are activated, everyone (including unauthorized parties) may be able to connect to the network and view the data flow.

Confidential corporate email messages, files containing competitive information and other company private information flow across wireless network during any company's normal operation. Intellectual property, competitive information, and company secrets can be exposed to anyone

with a wireless-enabled laptop that is parked outside the building. This problem can easily be solved by enabling the security features on the wireless access points. These security features encrypt the network traffic so that only authorized parties can read the data.

Encrypting Data at Rest

Data is also at risk when it is stored on media that is not in a completely controlled environment. Stolen and lost laptop computers plagued and embarrassed the IRS and NIH in 2006. Laptops can contain sensitive and confidential data. Laptops are portable and are easily transported from a secure environment such as the IRS offices to an unsecure environment such as the employees' favorite local lunchtime hang-out. The risks are high when the laptop contains thousands of social security numbers or trade secrets and the laptop is left behind on a chair at the restaurant.

Perhaps an even more ubiquitous and portable form of data storage is the USB flash drive. These lipstick-sized devices can carry gigabytes of valuable information. They are extremely convenient because they can be plugged into virtually any computer and used instantly making them a popular storage device. Because of their popularity and their small size, it is easy to see how these data storage devices could be misplaced or stolen. Since they are so convenient and ubiquitous, it is also easy to imagine that these little devices may contain lots of confidential information.

In November 2008, the U.S. Department of Defense (DOD) banned the use of USB storage devices after a device, infected with a worm affected many parts of the DOD networks. The ban lasted 15 months until the DOD decided that the USB devices were so pervasive that they had to continue their use. USB drives made it easy for DOD personnel to transfer large amounts of data to remote sites where network bandwidth was severely limited (e.g., ships at sea).

Sensitive, confidential data being transmitted or transported outside of secured, controlled environments are vulnerable to accidental or malicious exposure. Encrypting the data in transit and at rest prevents the data from being read or modified by unauthorized entities. Encryption is the last line of defense when the laptop containing trade secrets is lost or when electronic files are intercepted while being transferred across the Internet.

Customer Demand for Encryption

Today, many employees are able to work remotely from home offices or while travelling hundreds or thousands of miles away from their corporate email, file and web servers. These employees rely heavily on the virtual private network (VPN) software that enables secure communica-

tions between the remote location and the corporate servers. The VPN enable employees to connect to company compute resources as securely as if the client computer were hard-wired into the RJ-11 jacks in the corporate offices. The VPN encrypts the network traffic from the employee's computer to the company servers so that no one can decipher the messages and transactions that are being transferred.

Customers today also routinely use encryption technologies. Customer placing online orders enter their name, address, phone number, and credit card information into their "shopping cart" web page and press the "submit" button. The customer probably barely notices that the universal resource locator (URL) used for that web page starts with "https" rather than the more common "http". Hypertext Transport Protocol (HTTP) is the network protocol that enables web browsers such as Microsoft's Internet Explorer or Mozilla's Firefox to interact with application software running on remote servers. Information transferred between the user's client computer and the web servers use the international HTTP standard. To secure the transfer of confidential data such as credit card numbers, the Hypertext Transfer Protocol - Secure (HTTPS) is used. HTTPS combines HTTP with Secure Socket Layer/Transport Layer Security (SSL/TLS) cryptographic protocols to encrypt the communications between the web browsers and the web servers. With HTTPS, customers can be assured that credit card and other sensitive information cannot be stolen by a maleficent since the encrypted data will be unintelligible except to those with the proper authorization.

Use of encryption technologies such as VPN and HTTPS is commonplace by consumers and businesses everywhere. E-commerce has become the backbone of business transactions in the 21st century and encryption enables these transactions to occur securely and reliably.

Good business practice dictates the use of encryption to protect sensitive and confidential data. However, due to the publicity around some extensive data breaches, there has been an outcry for greater government oversight and regulation to allay the public's concerns. Identity theft and privacy concerns have caused legislators to enact regulations to protect consumer data, and in the event of an accidental or malicious breach, that affected citizens are notified.

Identity theft protection concerns grew to the point that in 2010, there were 46 states in the U.S. along with the District of Columbia, Puerto Rico and the U.S. Virgin Islands that had enacted data breach notification laws. These laws basically state that if a state's resident's "personal information" is lost or stolen, the responsible entity must report the incident to all potentially affected citizens. To demonstrate the strength of encryption, some of these laws such as California's Civil Code 1798.80-1798.84 contain "safe harbor" provisions whereby a responsible entity may be relieved of the obligation to disclose a data breach if the "personal information" is encrypted.

The U.S. Federal Government recognizes the need to have its agencies adhere to strong security and data protection standards. Not only is cryptographic technology seen as an important element to information security, all Federal agencies are mandated to use the FIPS 140 standard in designing and implementing cryptographic modules in information systems that they operate or are operated for them. Illustrating how important the FIPS 140 standard is viewed, the Federal Information Security Management Act (FISMA) of 2002 [FISMA] eliminated any provisions to waive the mandatory FIPS 140 validation. FIPS 140 precludes the use of un-validated cryptography for the cryptographic protection of sensitive data within Federal government systems. Un-validated cryptography is viewed as providing no protection to the data, as if it were the same as unprotected plaintext.

Value of FIPS 140

Why does the FIPS 140 standard exist and what purpose does it serve? Product vendors will develop cryptographic technologies to protect data. They will implement known, trusted algorithms. They will test their products to their corporate standards and make assertions that their product is "the most secure in the industry" or "meets industry standards." How can customers know for sure what they are purchasing will perform as advertised and as expected? How can they have confidence that the vendor claims are valid? Without some proof, customers would have to take the vendor's word that their claims are true. The FIPS 140 standards and the Cryptographic Module Validation Program (CMVP) provide value to customers by having independent third-parties validate vendor claims against the internationally-accepted FIPS 140 standards.

Customers want confidence that the products they purchase and use will meet their security requirements. Product vendors may assert that they include cryptographic features in their products and employ secure development practices. The level of confidence (or assurance) customers gain from vendor assertions depends on how trustworthy the vendors are. Independent confirmation of those vendor claims by third-party validators can give customers even greater confidence. Customers can gain even more confidence if those independent, third-party validations are performed using open, international standards. Benefits of these types of validations include:

- Examination against recognized industry standard metrics and criteria so customers have some confidence that the measures are complete and relevant
- Standardized validation methods so that customers are guaranteed consistent, unbiased results

- Credibility of the third party is the basis for trusting their results. Third parties that use open processes for standards development and publication of results gain the broadest credibility

Cryptographic testing and validation standards provide a way to do uniform comparisons of products. Having these standards reduces confusion for the customer so that they are not faced with trying to compare products evaluated under different regimes and criteria.

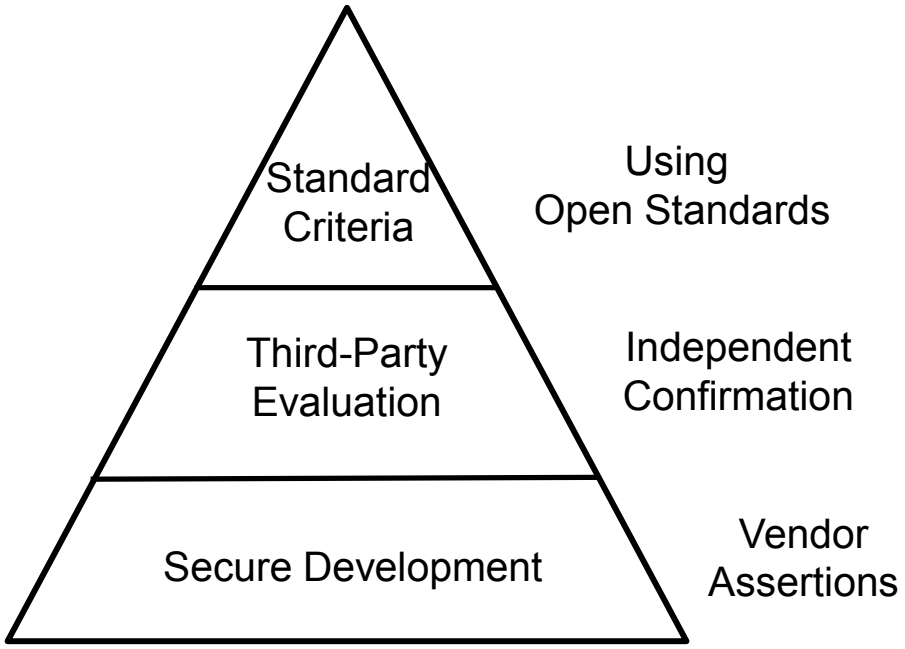


Figure 1: The Assurance Pyramid

The "assurance pyramid" in Figure 1 illustrates the increasing assurance or confidence customers can develop as different validation schemes are applied to assertions about the capabilities of cryptographic modules.

At the base, vendors implement cryptographic technologies in their products and assert that they meet certain standards or have certain capabilities in marketing or advertising claims. These vendors may apply good development practices and do their best to implement solid cryptographic algorithms. If the vendor is trustworthy, customers may be satisfied that their needs will be met.

The second level of assurance is third-party confirmation of vendor claims. This level can provide customers with even greater confidence since this confirmation comes from an independent validator. Depending on how well the third-party is recognized for conducting thorough and accurate validations, the customer may have greater confidence that the

cryptography has been developed properly and that the implementation will be free of obvious flaws.

Perhaps the highest level of customer confidence can be gained by the third level of assurance – validation by an independent third-party using open, recognized standards. Open standards allow a broad technical community to contribute to the development of a robust, effective, and realistic set of standards. Customers can gain confidence that a great deal of scrutiny has been placed upon the development of these standards. Customers also have the opportunity to check that the standards will meet their needs. The best standards also include a set of test or validation criteria so that not only is the cryptographic module features well-defined, the methods used to validate them is also specified.

Summary

Encryption has been proven over time to be an effective tool to protect data. Consumers and enterprises have grown to depend on encryption to protect their online transactions and data. Correct implementation and confidence in encryption technologies are important to the continued success of the commercial use of the Internet. Cryptographic module validation programs such as FIPS 140 serve to provide users with a level of confidence that the encryption technologies they use meet industry standards.

Chapter 4: Basic Applied Cryptography

There are a number of the several widely-recognized reference texts available today that cover the technical details of cryptographic algorithms. While the focus of those books is on the mathematics and science of cryptography, describing the gory (and sometimes boring) details of the wide variety of cryptographic techniques used throughout history, the primary purpose of this book is to educate the product developer about the requirements for the current FIPS 140 cryptographic module validation process. However, in order to understand the FIPS 140 validation process, it is necessary to have a basic understanding for the applicable cryptographic technologies recognized by the FIPS 140 standard. This chapter will give the reader that basic understanding using layman's terms and simplified examples.

Encrypting and Decrypting Data

Cryptographic data encryption is rooted in some complex mathematics, however the basic principle is that an algorithm (i.e. mathematical formula) is used to transform (or encode or encrypt) characters or sets of characters (e.g., a plaintext message) into some other form and another algorithm is used to decode (or decrypt) the message back into plaintext. Encryption provides protection of the confidentiality of the messages whereby only authorized recipients are able to read the encrypted messages. In this context, a message may be a message that is transmitted across a network or it can be some data stored on a disk.

A plaintext message can be thought of as nothing but a string of binary digits (bits). ASCII character representations are a common way to transform natural language characters into bits. The letter "A" for example, is represented in ASCII as a hexadecimal 41 or 0100 0001 in binary. The word "America" would then be represented as 41 6D 65 72 69 63 61 in hexadecimal and 0100 0001 0110 1101 0110 0101 0111 0010 0110 1001 0110 0011 0110 0001 in binary. Entering this string into an encoding algorithm results in an encoded bit string (ciphertext). A decoding algorithm and a decoding key are used to reverse the process and decode the ciphertext. Figure 2 illustrates the basic encoding and decoding process.

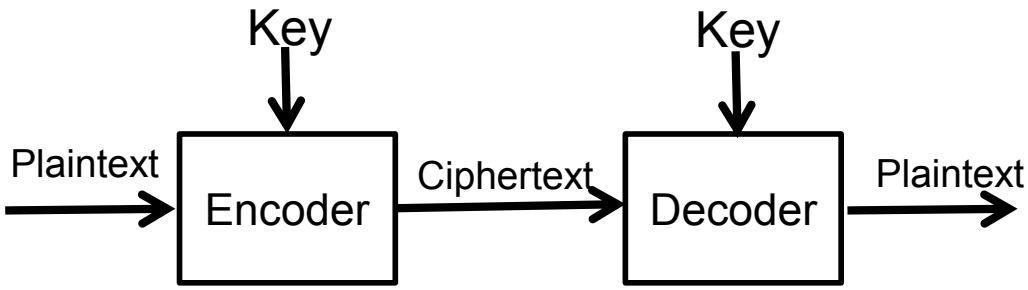


Figure 2: Encoding and Decoding

From a security perspective, it is safer to assume that the encoding and decoding algorithms will become known by attackers, so relying on the secrecy of the algorithms is not prudent. Recognizing this, the FIPS 140-approved algorithms are all documented as open standards and are readily available [CAVP]. Modern cryptographic techniques are so sophisticated that knowing the algorithm alone is not sufficient to decode an encoded message - a "key" must be used. Without the proper key, the encoded message is unintelligible. These "keys" are input parameters to randomize the output and provide the security to the algorithm. Keys have the added advantage that they can easily be changed, making the whole scheme scalable across many users.

A Word About Cryptographic Strength

Cryptographic algorithms are considered "strong" not because they are mathematically impossible to break, but because they are computationally prohibitive to break. Much of the mathematics behind cryptography involves number theory and complex computations. Computations are "expensive" – that is, they take time to compute, so the assumption is that an algorithm is "strong enough" if the computations necessary to break the algorithm are prohibitively expensive. The longer it takes to decrypt a message without knowing the key, the stronger the algorithm is considered to be. If an attacker takes literally years to decrypt an encoded message, it is likely that it would not be worth the effort.

FIPS 140 has selected a set of algorithms that are considered by experts to be strong given today's computing capabilities. Chapter 5: FIPS 140 Approved Algorithms will go into more details about each algorithm that has been approved for the FIPS 140 validation program.

Symmetric Key Algorithms

Figure 2 shows the generic message encoding and decoding process using keys. With symmetric key algorithms, the key used to encode the message is the same as the key used to decode the message, as illustrated

in Figure 3. Generally speaking, symmetric key algorithms are simpler and thus less computationally intensive than other algorithms (such as asymmetric algorithms) and are ideal for limited computing platforms such as smart cards or mobile devices. Symmetric key algorithms are also relatively fast, so securing real-time message transfers would be an appropriate application for a symmetric key algorithm.

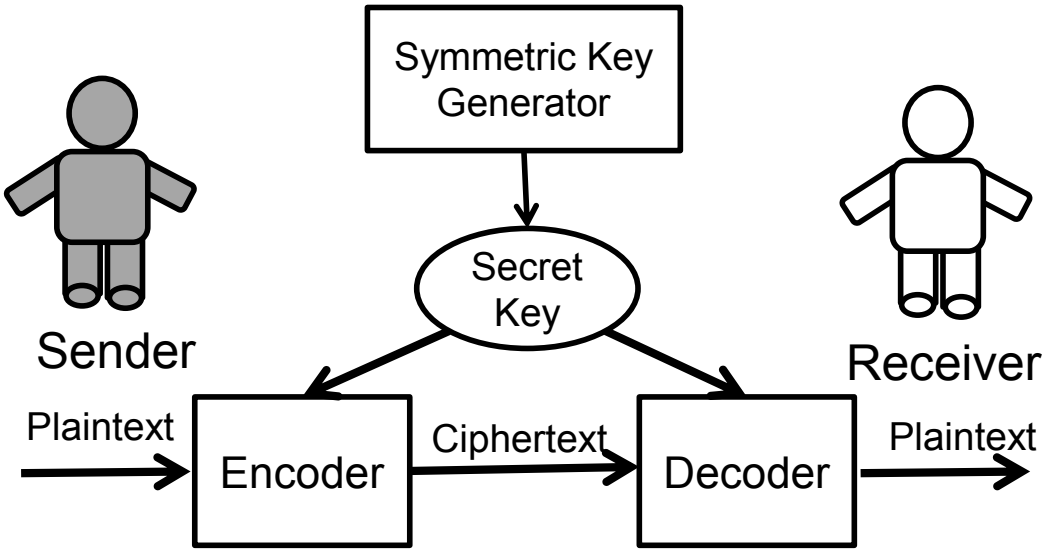


Figure 3: Symmetric Key Algorithm

The major drawback to symmetric key algorithms is that the encoding/decoding key must somehow be securely shared between the sender and the receiver. Asymmetric key algorithms were developed to overcome this shortcoming.

Asymmetric Key Algorithms

Where symmetric key algorithms use the same key for both encoding and decoding data, asymmetric key algorithms use one key for encoding and a different key for decoding. Asymmetric key algorithms are also known as public key algorithms because one key can be shared widely. The other private key must not be distributed. This eliminates the need for a secure mechanism to share keys as with symmetric key algorithms. Freedom from this limitation allows asymmetric methods to be more easily and more widely deployed.

Figure 4 illustrates the asymmetric key algorithm. First, the public key and paired private key are created by the key generator. While the two keys are related, the private key cannot be derived from the public key. The public key may be distributed, so anyone can use it to securely encode messages intended only for the holder of the private key. Only the private key can decode messages encoded using the public key.

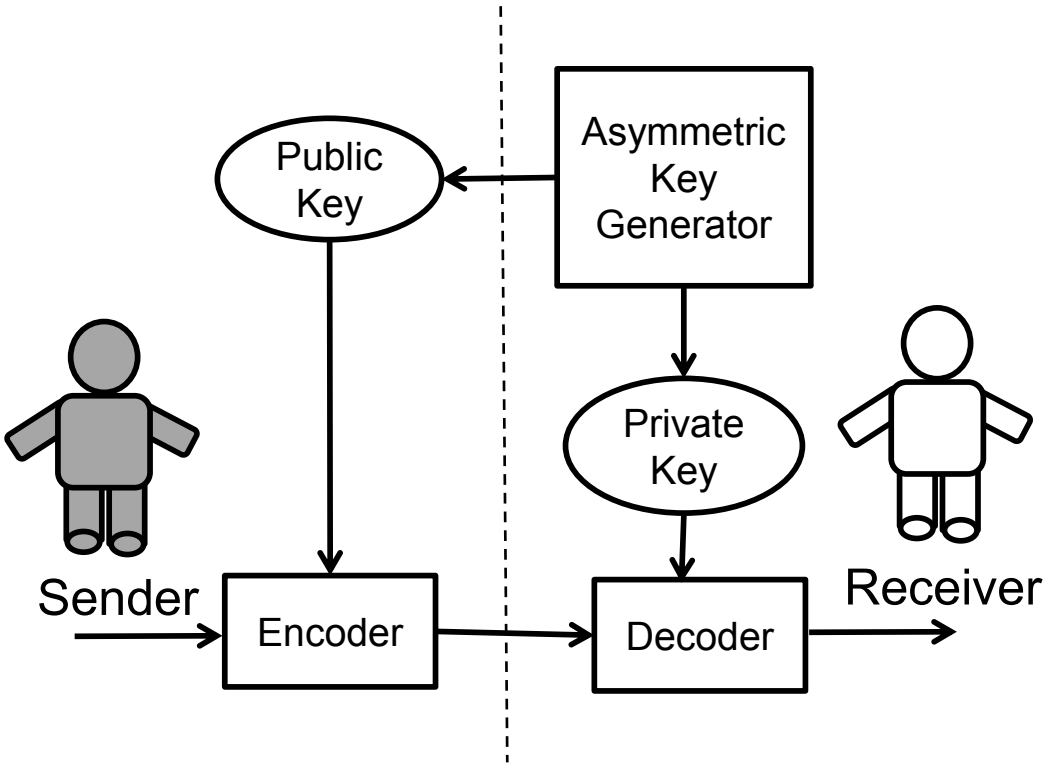


Figure 4: Asymmetric Key Algorithm

A drawback to asymmetric algorithms is that they are more compute-intensive and take longer to operate compared to symmetric key algorithms. For this reason, asymmetric key algorithms may be appropriate for securing email messages where servers and desktops have the necessary computing power and email delivery is less time-sensitive.

Hash Functions

Encrypting messages ensures the confidentiality of the messages. In some applications, all that is needed is to know that the integrity of the message content has been maintained – that is, no one has tampered with the contents of the message. An example of a good application of a cryptographic hash function is verifying a correct and complete file transfer. Hash functions provide message integrity. Figure 5 illustrates how a hash function generates a unique number (hash value or message digest) from a message. The hash function is designed such that the original message cannot be obtained by the hash value - that is, the hashing function is a "one-way" function. The hash value is sent with the message to the receiver. The receiver will re-generate the hash value using the hash function and compare the newly-generated hash value with the hash value

that was delivered with the message. If the two values are not equal, then the message was modified in transit.

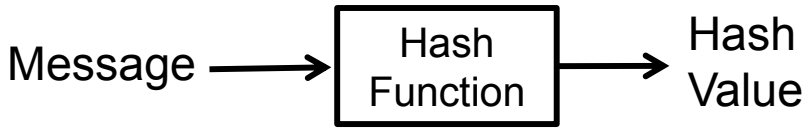


Figure 5: Hash Function

There is no guarantee that if the two hash values were equal that the message was not modified because the hash function is publicly known and the transmitted hash value is unprotected. Someone could intercept the message, modify the message, create a new hash value and send the modified message with the modified hash value to the original recipient. Hash functions provide no authentication.

Message Authentication Code

Message Authentication Code (MAC) schemes apply a secret (symmetric) key to the transmitted message. This provides the authentication that the message originated from the expected sender. Figure 6 illustrates the MAC scheme mechanism. The sender sends not only the plain text message to the receiver, but a tag is also sent. The tag is generated using the plaintext and the shared secret key as inputs to the MAC algorithm. The receiver then re-generates the tag using the plaintext and the secret key. If the received tag and the re-generated tag are identical, then the plaintext message was not modified and was sent by an authorized entity.

Hash Message Authentication Code (HMAC) appends a symmetric key to the plaintext message prior to generating the hash value. The receiver verifies the originator by re-generating the hash value using the secret key.

Cipher-Block Chaining-Message Authentication Code (CBC-MAC) method encrypts a message using a symmetric key algorithm in cipher-block chaining mode (CBC mode). The last cipher block is used as the message authentication code (MAC). The plaintext and the MAC are both sent. The receiver encrypts the plaintext using the symmetric key to re-generate the last cipher block and compares it to the MAC.

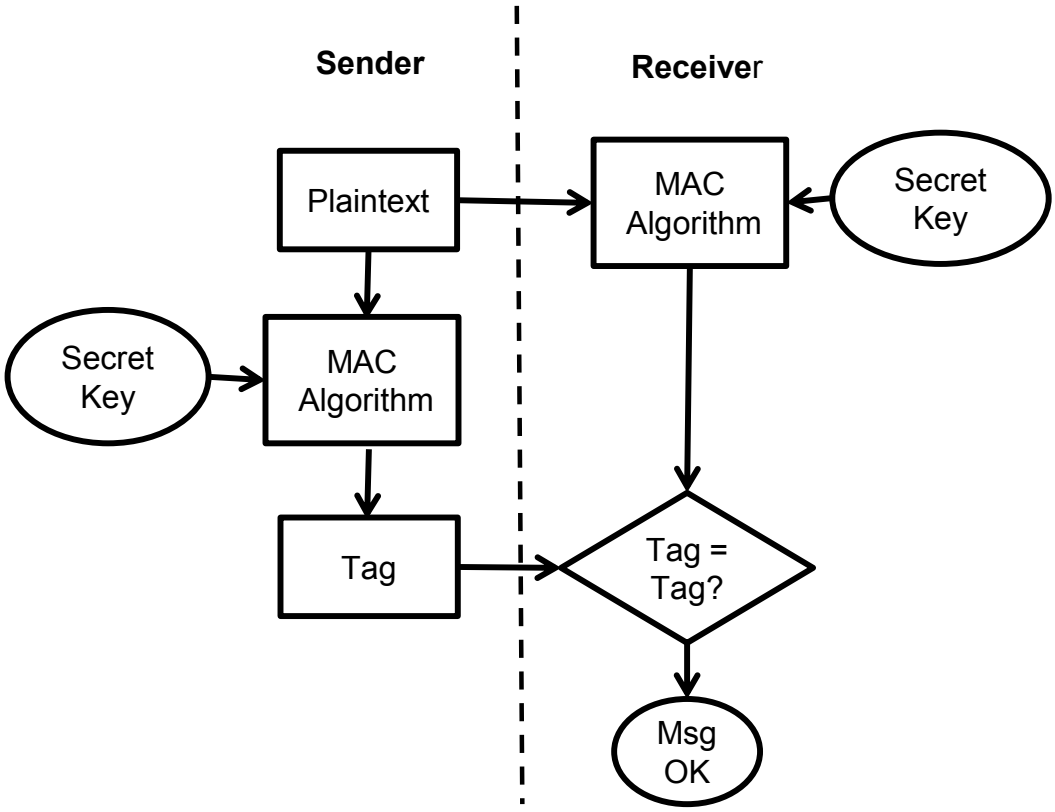


Figure 6: Message Authentication Mechanism

Encrypting messages in fixed-length blocks is called cipher block encryption. Cipher-Block Chaining (CBC) uses a method that causes the decryption of a block of ciphertext to depend on all the preceding ciphertext blocks. A single bit error in a given ciphertext block invalidates the decryption of all subsequent blocks. Rearrangement of the order of the ciphertext blocks corrupts the decryption. This makes it an effective means to detect message tampering.

Digital Signatures

A digital signature is a hash value that has been encrypted using an asymmetric algorithm private key. As illustrated in Figure 7, a hash value is computed on the plaintext message using a one-way hash function. The hash value is then encrypted using a private key. The plaintext message, along with the encrypted key is send to the receiver. The receiver then computes the hash value of the plaintext, decrypts the encrypted hash value using the public key, and compares the two values. If the two values are the same, the receiver can be assured that the message came from the expected sender and has not been modified in transit.

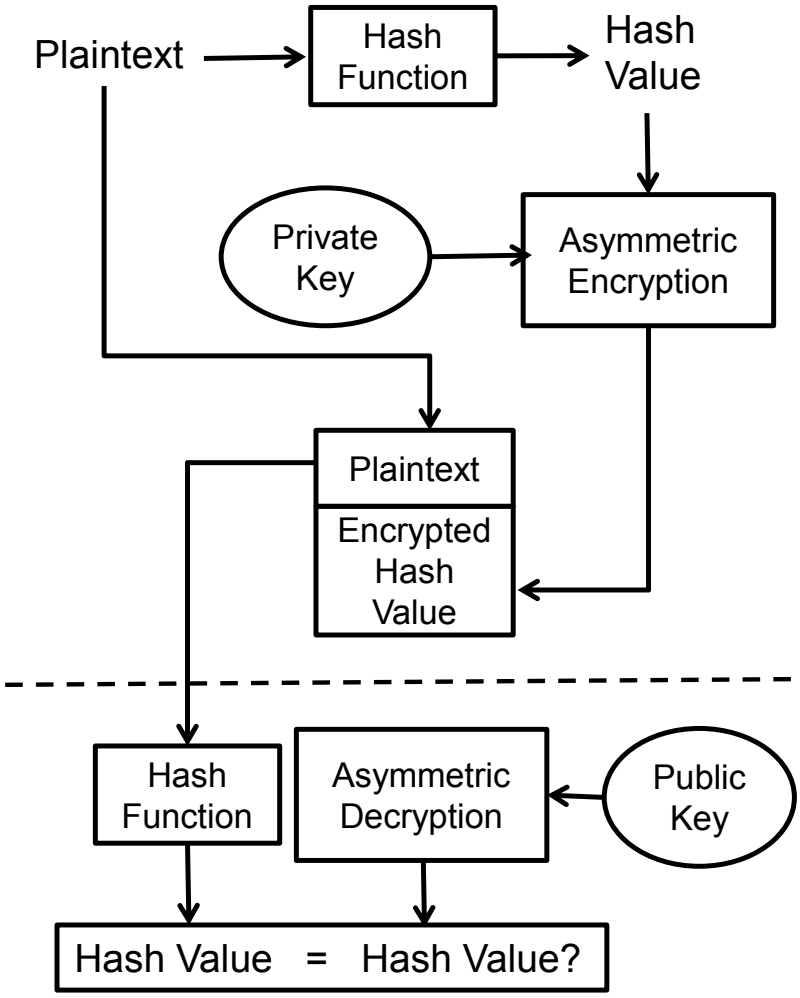


Figure 7: Digital Signature

Digital signatures have the additional benefit of non-repudiation over message authentication codes. Because only one authorized sender can have the asymmetric private key and because the digital signature can only be generated using the private key, the receiver can be assured that the message was sent by only the authorized entity.

Summary of Message Security Options

As discussed so far in this chapter, there are several options to secure messages (and data at rest). Table 1 is a summary of those options and the security features that each provides:

- Encryption provides message confidentiality
- Hashing provides message integrity
- Message authentication provides integrity and authentication

- Digital signatures provide integrity, authentication, and non-repudiation

	Confidentiality	Integrity	Authentication	Non-Repudiation
Encryption	X			
Hashing		X		
MAC		X	X	
Digital Signatures		X	X	X

Table 1: Cryptographic Features

Key Generation and Establishment

Since the security and strength of a cryptographic algorithm depends upon the key, key generation and key establishment are critical factors to the quality of the overall cryptographic scheme.

Random Number Generation

Preventing an attacker from guessing cryptographic keys is critical to the success of the cryptographic algorithm. Attackers obtaining secret keys in symmetric key algorithms or private keys in asymmetric algorithms would allow them to read and modify encrypted messages rendering the communications useless. Key generation mechanisms must make it difficult for anyone to guess the keys.

Randomness is an important factor in generating strong keys for cryptographic algorithms. Since keys must be generated from a finite set of possibilities (based on key length), the key generation mechanism must randomly select keys from that set. For example, if the key length is 128 bits long, there are 2^{128} possible keys that can be generated. Strong key generation mechanisms will randomly select a key from the 2^{128} possibilities.

Random number generators are used to help "seed" or start the key generation mechanism. Modern random number generators rely upon entropy or some physical phenomenon that is unpredictable. Some random number generators use ambient air temperature or biometrics as entropy input.

Once a random number has been generated, each key generation algorithm uses its own method for creating the key from the set of all possible keys.

Key Establishment Schemes

As was mentioned earlier in this chapter, symmetric key algorithms have the advantage of being computationally faster and thus requiring less computing power. However, the disadvantage to these algorithms is that the shared, secret key must somehow be distributed in a secure manner in order to be practical. Secret keys can be distributed securely by using a hybrid encryption method that employs asymmetric key algorithms.

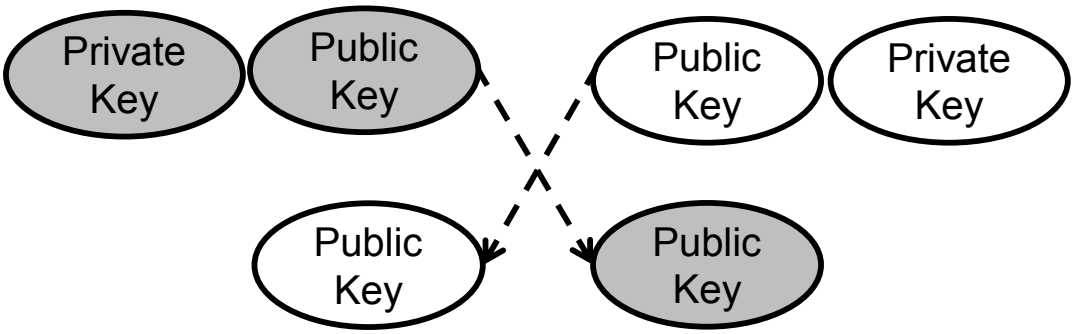


Figure 8: Asymmetric Key Sharing

Figure 8 shows the public and private keys of two parties wishing to share encrypted information. Each party provides the other party with their asymmetric public key.

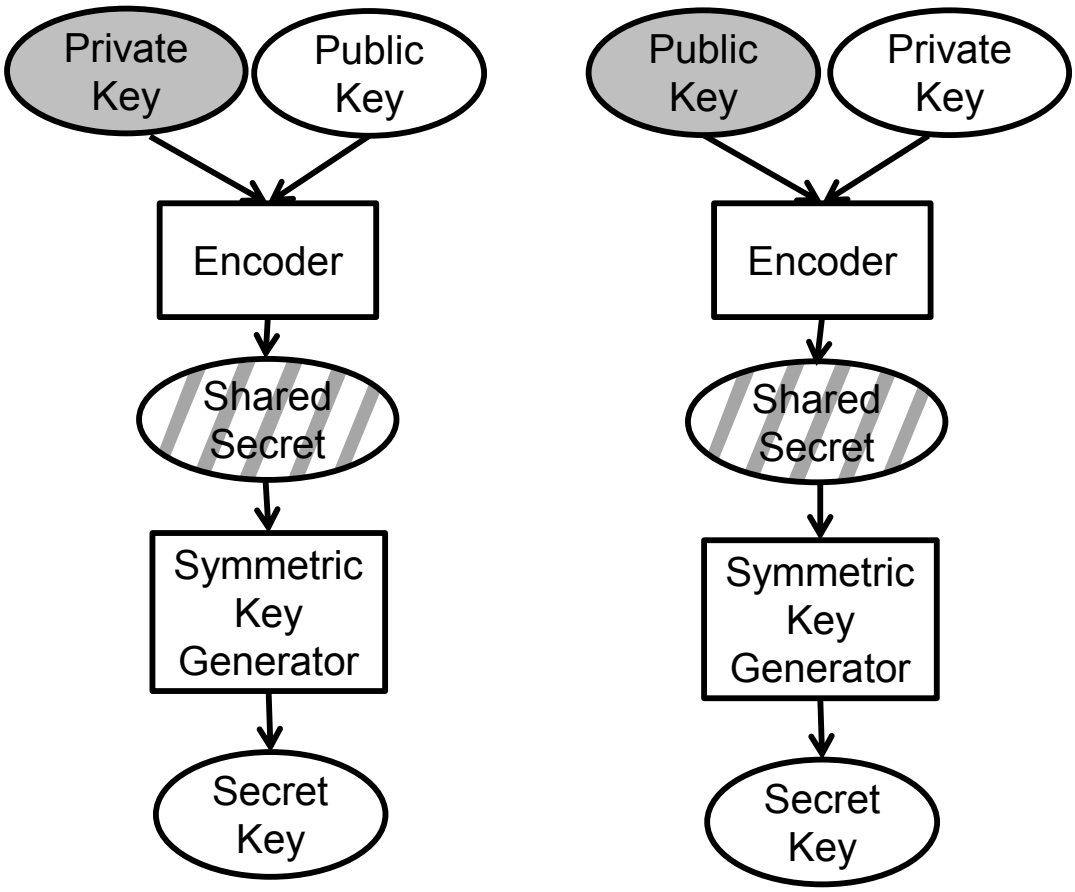


Figure 9: Key Establishment

Figure 9 shows each party using the other party's public key plus their own private key to generate a "shared secret." That shared secret, in turn, is used to generate a symmetric key or secret key. Now that both parties have the secret key, they may communicate with messages encrypted with the symmetric key algorithm.

Cryptography Vulnerabilities

Within each category, the National Institute of Standards and Technology (NIST) approve only a small set of cryptographic algorithms for FIPS 140 validation. The list of approved algorithms has changed over the years as vulnerabilities were discovered in the older ones and new, stronger, more secure algorithms took their places.

Older cryptographic algorithms are replaced as vulnerabilities or weaknesses are discovered. Oftentimes these weaknesses are theoretical mathematical proofs, while others are actual demonstrations of algorithms being broken. In 1999, Distributed.Net and the Electronic Frontier Foundation demonstrated that the then-popular Data Encryption Standard (DES)

algorithm could be broken in a matter of hours [RSA DES]. They used a network of nearly 100,000 distributed computers to perform the massive number of calculations necessary to decrypt a DES-encrypted message. As computing power increases and attack techniques grow in sophistication, older algorithms need to be upgraded or replaced in order to maintain the highest levels of security.

Implementation flaws are a major cause for concern with cryptographic modules. Many times cryptographic modules are broken because of software bugs or weak key generation. According to NIST, in 2002 security flaws were discovered during testing in 88 out of 332 algorithms (or 26.5%). By 2010, the error rate had dropped to approximately 10%.

Summary

There are many facets to cryptography including encryption, decryption, hashing, message authentication, digital signatures and key generation. The FIPS 140 reference standards for certain aspects of cryptography. This chapter has provided a basic overview of the cryptographic topics relevant to FIPS 140.

The next set of chapters contained within Part 2 of this book delves into the details of the FIPS 140 standards and the cryptographic algorithm and module validation programs.