Information Security Notes

Cybersecurity is the protection of information that is stored, transmitted, and processed in a networked system of computers, other digital devices, and network devices and transmission lines, including the Internet. Protection encompasses confidentiality, integrity, availability, authenticity, and accountability.

As subsets of cybersecurity, we can define the following:

■ **Information security:** This term refers to preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

■ **Network security:** This term refers to protection of networks and their service from unauthorized modification, destruction, or disclosure

■ **Confidentiality:** This term covers two related concepts:

**— Data**1 **confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

**Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

**— Data integrity:** Assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.

**Availability:** Assures that systems work promptly and service is not denied to authorized users.

**Security attack** – Any action that compromises the security of information owned by an

organization.

**Security mechanism** – A mechanism that is designed to detect, prevent or recover from a

security attack.

**Security service** – A service that enhances the security of the data processing systems and the

information transfers of an organization.

**Confidentiality:** Ensures that the information in a computer system a n d transmitted

information are accessible only for reading by authorized parties.

E.g. Printing, displaying and other forms of disclosure.

Confidentiality is the protection of transmitted data from passive attacks.

**Authentication:** Ensures that the origin of a message or electronic document is correctly

identified, with an assurance that the identity is not false.

**Integrity:** Ensures that only authorized parties are able to modify computer system assets and

transmitted information. Modification includes writing, changing status, deleting, creating

and delaying or replaying of transmitted messages.

**Non repudiation**: Requires that neither the sender nor the receiver of a message be able to deny

the transmission.

**Nonrepudiation**

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message

**Access control**: Requires that access to information resources may be controlled by or the target system.

**Availability**: Requires that computer system assets be available to authorized parties when needed. A system is available if it provides services according to the system design whenever users request them)

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

■ Attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

Two types of passive attacks are the release of message contents and traffic analysis. A second type of passive attack, traffic analysis, is subtler. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. the emphasis in dealing with passive attacks is on prevention rather than detection.

An active attack attempts to alter system resources or affect their operation.

**Active attacks** involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service.

A **masquerade** takes place when one entity pretends to be a different entity.

**Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

**Data modification** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

The **denial of service** prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

A masquerade can take the form of a man-in-the-middle attack (Figure 1.3c). In this type of attack, the attacker intercepts masquerades as the client to the server and as the server to the client. More generally, it can be used to impersonate the two ends of a legitimate communication. Another form of masquerade is illustrated in Figure 1.3d. Here, an attacker is able to access server resources by masquerading as an authorized user.

Figure 1.3e illustrates the replay attack. As in a passive attack, the attacker does not disturb the information flow between client and server, but does capture client message. The attacker can then subsequently replay any client message to the server.

Figure 1.3d also illustrates denial of service in the context of a client/server environment. The denial of service can take two forms: (1) flooding the server with an overwhelming amount of data; and (2) triggering some action on the server that consumes substantial computing resources.

The **authentication** service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

**Access Control**

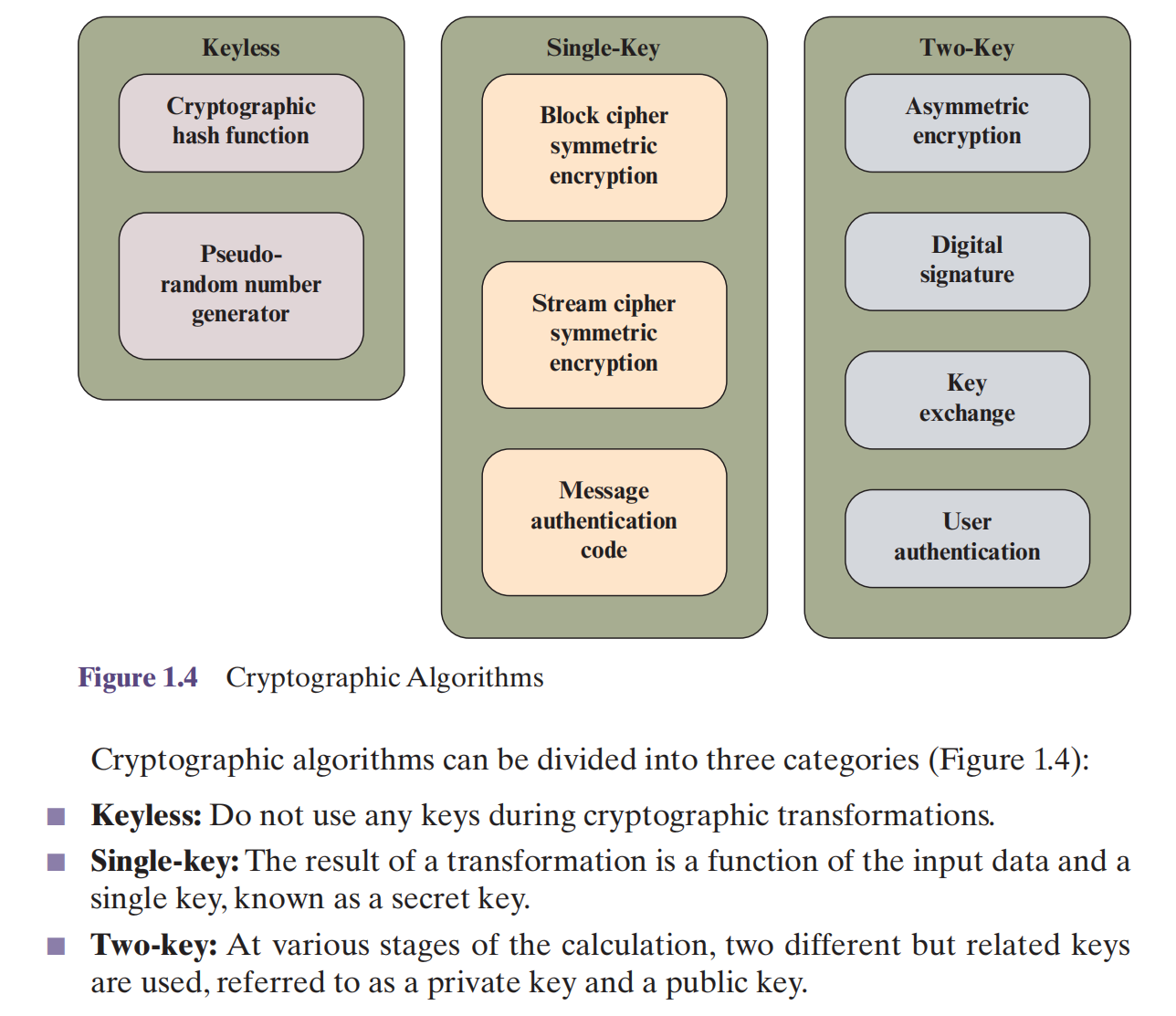
In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.Because the integrity service relates to active attacks, we are concerned with detection rather than prevention.

**Cryptographic algorithms:** We can distinguish between reversible cryptographic mechanisms and irreversible cryptographic mechanisms. A reversible cryptographic mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible cryptographic mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

**Digital signature:** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery

Notarization: The use of a trusted third party to assure certain properties of a data exchange.

Cryptography is a branch of mathematics that deals with the transformation of data.



A hash function turns a variable amount of text into a small, fixed-length value called a *hash value, hash code*, or *digest*. A **cryptographic hash function** is one that has additional properties that make it useful as part of another cryptographic algorithm, such as a message authentication code or a digital signature.

Encryption algorithms that use a single key are referred to as **symmetric encryption algorithms**

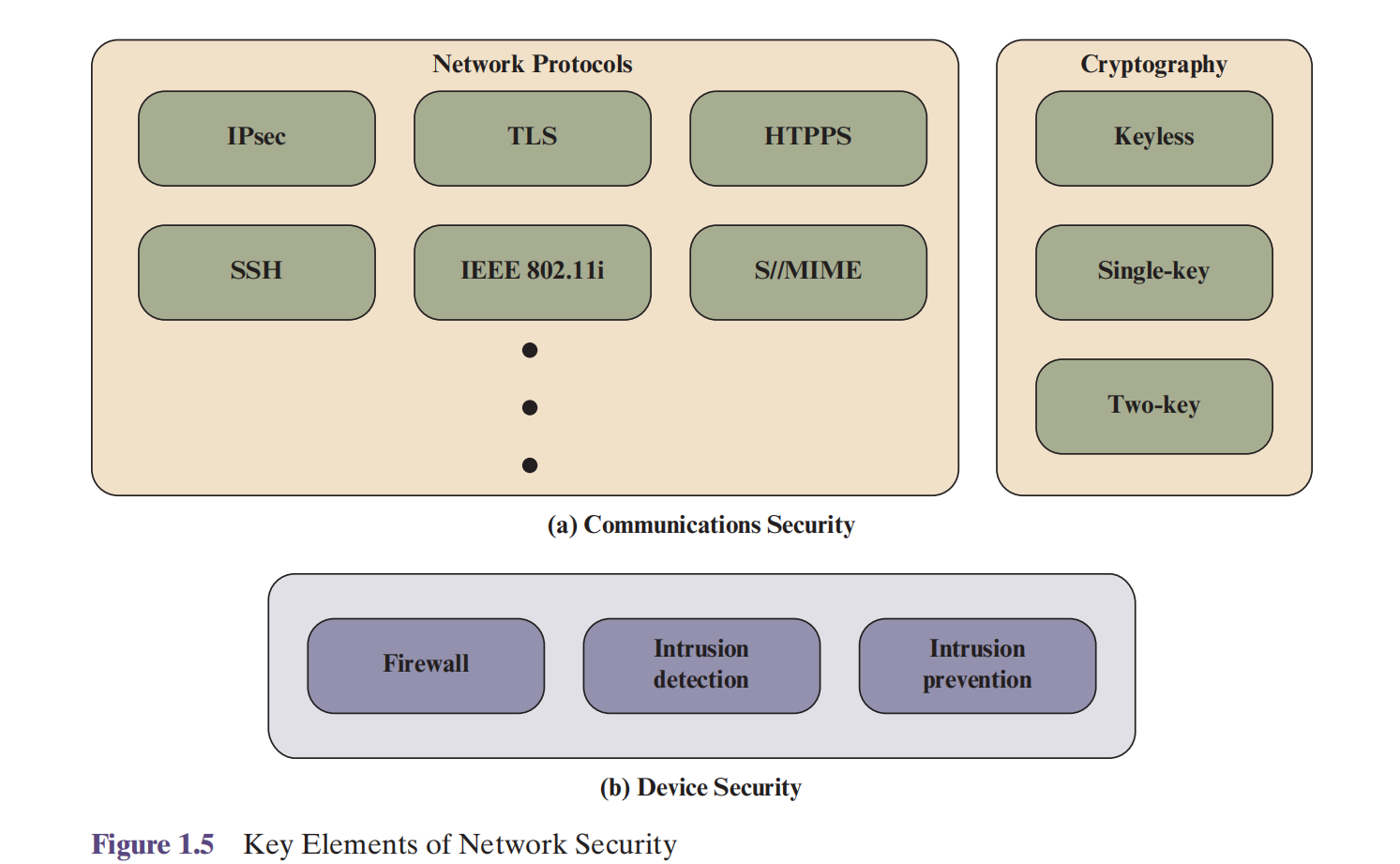
**Block cipher:** A block cipher operates on data as a sequence of blocks. A typical block size is 128 bits. In most versions of the block cipher, known as modes of operation, the transformation depends not only on the current data block and the secret key but also on the content of preceding blocks.

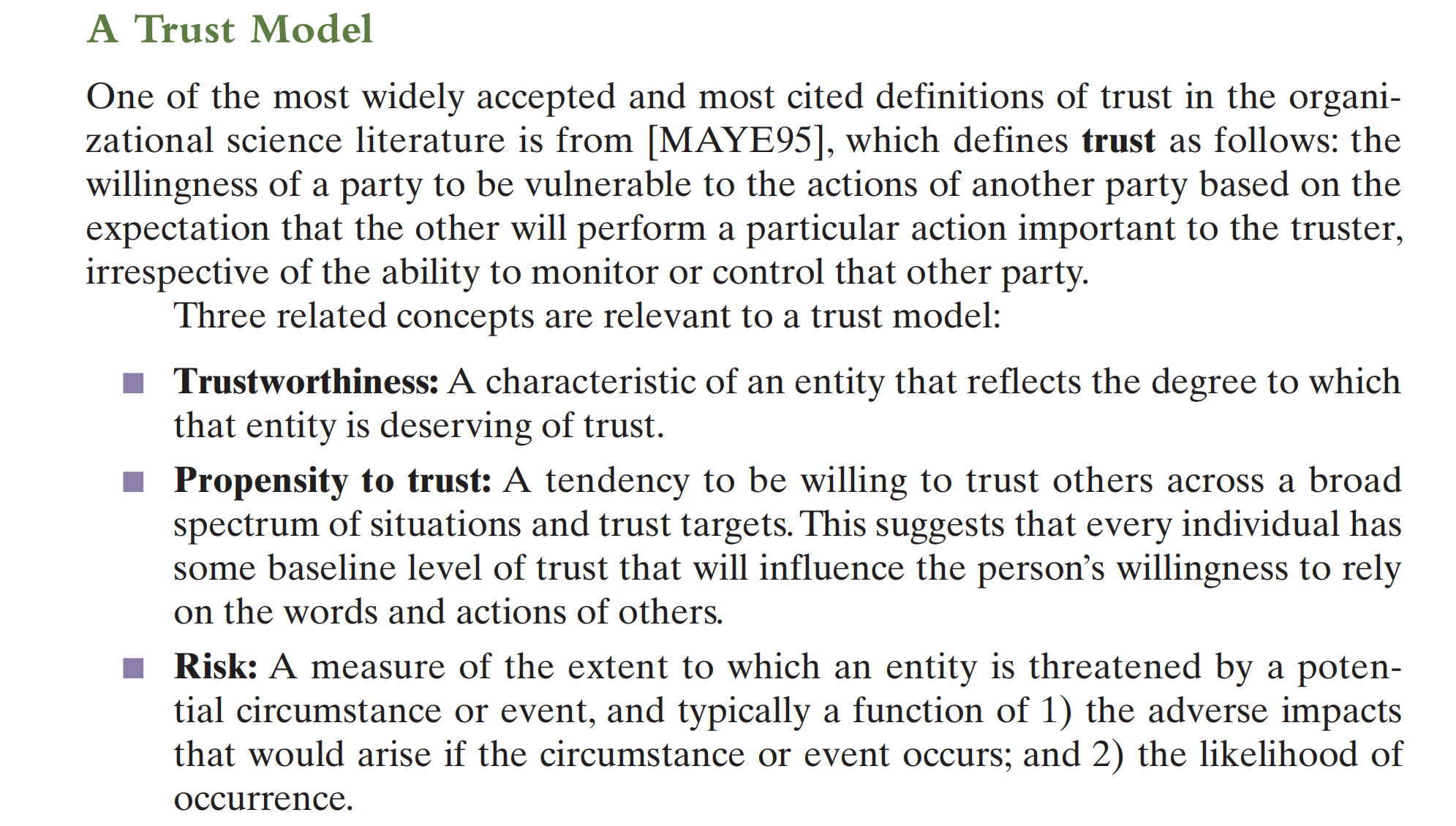
■ **Stream cipher:** A stream cipher operates on data as a sequence of bits. Typically, an exclusive-OR operation is used to produce a bit-by-bit transformation. As with the block cipher, the transformation depends on a secret key.

Another form of single-key cryptographic algorithm is the **message authentication code** (MAC). A MAC is a data element associated with a data block or message. The MAC is generated by a cryptographic transformation involving a secret key and, typically, a cryptographic hash function of the message. The MAC is designed so that someone in possession of the secret key can verify the integrity of the messageEncryption algorithms that use two keys are referred to as **asymmetric encryption algorithms.**Asymmetric encryption has a variety of applications. One of the most important is the **digital signature algorithm**. A digital signature is a value computed with

a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data’s origin and integrity. Typically, the signer of a data object uses the signer’s private key to generate the signature, and anyone in possession of the corresponding public key can verify that validity of the signature.

**Key exchange** is the process of securely distributing a symmetric key to two or more parties. **User authentication** is the process of authenticating that a user attempting to access an application or service is genuine and, similarly, that the application or service is genuine





An original message is known as the **plaintext**, while the coded message is called the **ciphertext**.

The process of converting from plaintext to ciphertext is known as **enciphering** or **encryption**;

restoring the plaintext from the ciphertext is **deciphering** or **decryption**.

The many schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme

is known as a **cryptographic system** or a **cipher**.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of

**cryptanalysis**. Cryptanalysis is what the layperson calls “breaking the code.”

The areas of cryptography and cryptanalysis together are called **cryptology**.

A symmetric encryption scheme has five ingredients: Plaintext, Ciphertext, encryption algorithm, decryption algorithm, secret key.

We assume that it is impractical to decrypt a message on the basis of the ciphertext *plus* knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret. This feature of symmetric encryption is what makes it feasible for widespread use.

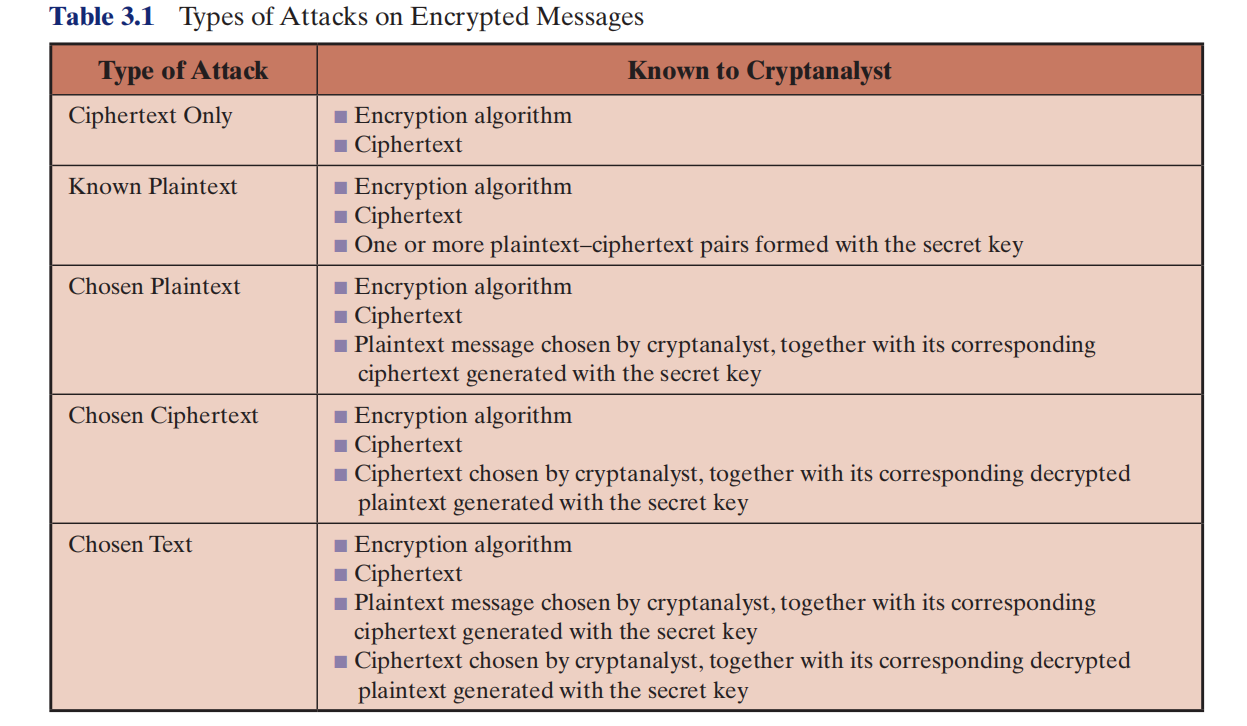
Cryptanalysis and Brute-Force Attack

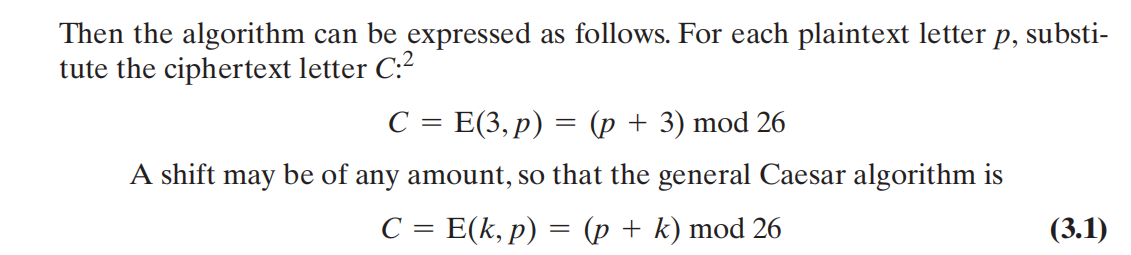
Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

■ Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

■ Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

That is, if there are *X* different keys, on average an attacker would discover the actual key after *X*/2 tries.





Plaintext is always in lowercase; ciphertext is in uppercase;

a **monoalphabetic substitution cipher**, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.3 The Playfair algorithm is based on the use of a 5 \* 5 matrix of letters constructed using a keyword.

A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. Examples of classical stream ciphers are the autokeyed Vigenère cipher and the Vernam cipher .

A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used

Identification, as you just learned, is simply an assertion of who we are.

This may include who we claim to be as people, who a system claims to

be over the network, or who the originating party of an email claims to

be.

In information security, authentication is the set of methods used to

establish whether a claim of identity is true. Note that authentication

does not decide what the party being authenticated is permitted to do;

this is a separate task, known as authorization

Let’s return to the ATM example because it illustrates multifactor

authentication well. In this case, you use something you know (your

PIN) and something you have (your ATM card). Your ATM card serves

as both a factor for authentication and a form of identification. Another

example of multifactor authentication is writing checks. In this case,

you’re using something you have (the checks themselves) and something

you do (signing them).

Mutual authentication is an authentication mechanism in which both

parties in a transaction authenticate each other. In a man-in-the-middle attack, the attacker inserts himself between the client and the server. The attacker then impersonates the server to the client and the client to the server

Passwords

Although they’re only a single factor of authentication, passwords can

represent a relatively high level of security when constructed and

implemented properly

You can use biometric systems in two ways. You can use them to

verify the identity claim someone has put forth, as discussed earlier, or

you can reverse the process and use biometrics as a method of

identification. Processing the characteristic may also include noting elements that appear at certain parts of the image, known as minutiae. You can use the minutiae later to match the characteristic to the user

Biometric factors are defined by seven characteristics: universality,

uniqueness, permanence, collectability, performance, acceptability, and

circumvention.

Universality means you should be able to find your chosen biometric

characteristic in the majority of people you expect to enroll in the

system.

Uniqueness is a measure of how unique a characteristic is among

Individuals.

Permanence tests how well characteristic resists change over time

and with advancing age.

Collectability measures how easy it is to acquire a characteristic.

Circumvention describes how easy it is to trick a system by using a

falsified biometric identifier.

The false

acceptance rate (FAR) and false rejection rate (FRR) are two of these. 6 FAR

measures how often you accept a user who should be rejected. This is

also called a false positive. FRR measures how often we reject a legitimate

user and is sometimes called a false negative.

You want to avoid both of these situations in excess. You should aim for a balance between the two error types, referred to as an equal error rate (EER). If you plot both the FAR and the FRR on a graph, as I’ve done in Figure 2-4, the EER marks the point where the two lines intersect. We sometimes use EER as a measure of the accuracy of biometric systems.

The majority of the encryption algorithms currently in use are block ciphers. Although block ciphers are often slower than stream ciphers, they tend to be more versatile. Since block ciphers operate on larger blocks of the message at a time, they’re usually more resource intensive and more complex to implement. They’re also more susceptible to errors in the encryption process. For example, an error in block cipher encryption would render a large segment of data unusable, whereas in a stream cipher, an error would corrupt only a single bit.

DES is a block cipher that uses a 56-bit key

AES

(Advanced Encryption Standard)

AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications.

**FINITE FIELD ARITHMETIC(Syllabus a NAI)**

In AES, all operations are performed on 8-bit bytes. In particular, the arithmetic

operations of addition, multiplication, and division are performed over the finite field

GF(28 ).

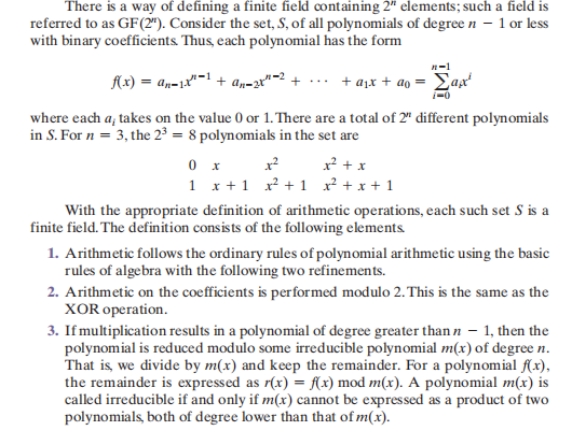
In essence, a **field** is a set in which we can do addition, subtraction, multiplica

tion, and division without leaving the set. Division is defined with the following rule:

*a*/*b* = *a*(*b*-1 ). An example of a **finite field** (one with a finite number of elements) is

the set Z*p* consisting of all the integers {0, 1, c , *p* - 1}, where *p* is a prime num

ber and in which arithmetic is carried out modulo *p*.



AES STRUCTURE

**Plain-text**

1. The cipher takes a plain-text block size of 128 bits, or 16 bytes.
2. The key length can be 16, 24,or 32 bytes (128, 192, or 256 bits). The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length.
3. The input is a single 128-bit block. This block is depicted as a 4 \* 4 square matrix of bytes.
4. This block is copied into the **State** array, which is modified at each stage of encryption or decryption.
5. After the final stage, **State** is copied to an output matrix.

**Key**

1. The key is depicted as a square matrix of bytes.
2. This key is then expanded into an array of key schedule words.
3. Each word is four bytes, and the total key schedule is 44 words for the 128-bit key.

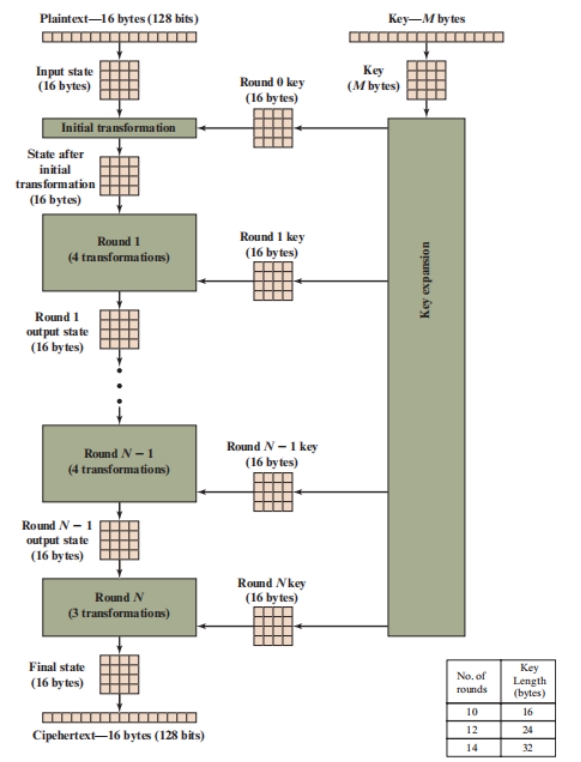
# Note that the ordering of bytes within a matrix is by column.

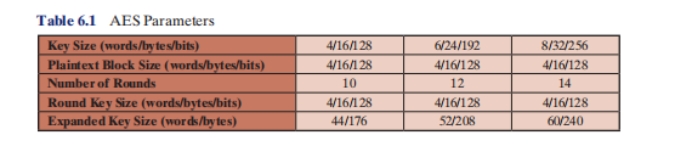
So, for example, the first four bytes of a 128-bit plaintext input to the encryption cipher occupy the first column of the **in** matrix, the second four bytes occupy the second column, and so on. Similarly, the first four bytes of the expanded key, which form a word, occupy the first column of the **w** matrix.

The cipher consists of *N* rounds, where the number of rounds depends on the

key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32-byte key .

The first *N* - 1 rounds consist of four distinct transformation functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey.The final round contains only three transformations.





Detailed Structure

* It is not a Feistel structure AES instead processes the entire data block as a single matrix during each round using substitutions and permutation.

* The key that is provided as input is expanded into an array of forty-four 32-bit words, **w**[*i*]. Four distinct words (128 bits) serve as a round key for each round;

* Four different stages are used, one of permutation and three of substitution:

■ **Substitute bytes:** Uses an S-box to perform a byte-by-byte substitution of

the block.

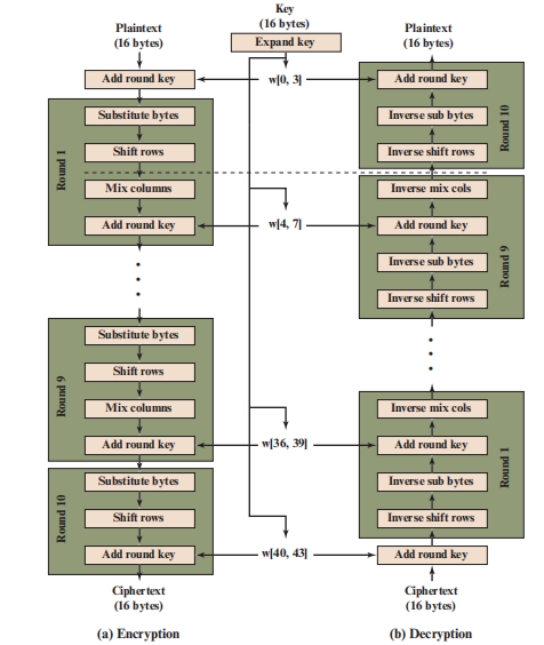
■ **ShiftRows:** A simple permutation.

■ **MixColumns:** A substitution that makes use of arithmetic over GF(28 ).

■ **AddRoundKey:** A simple bitwise XOR of the current block with a portion

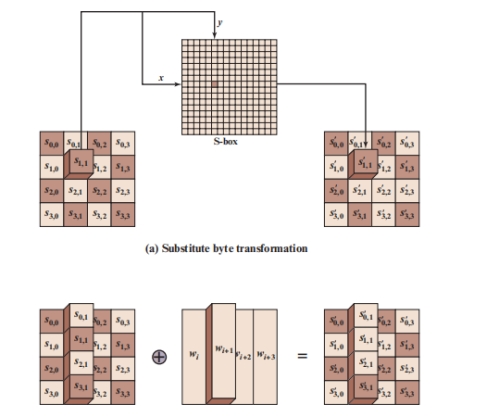
of the expanded key.

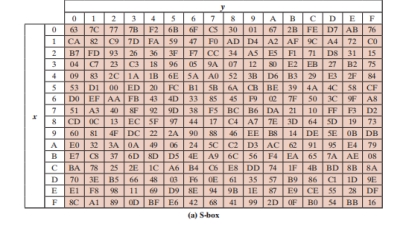
* Only the AddRoundKey stage(a form of Vernam cipher) makes use of the key.
* Any other stage, applied at the beginning or end, is reversible without knowledge of the key and so would add no security

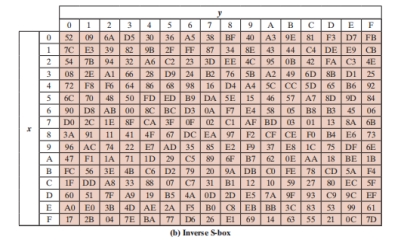


**Substitute Bytes Transformation**

Each individual byte of **State** is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value.





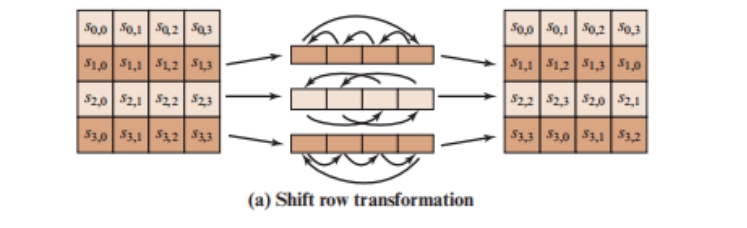


**ShiftRows Transformation**

The first row of **State** is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed.

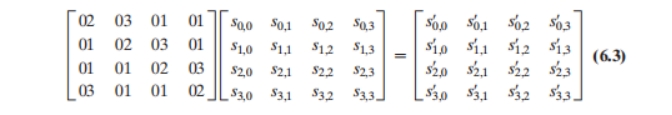
**ShiftRow** -Left/right circular shift.

**InverseShiftRow** -Opposite direction circular shift.



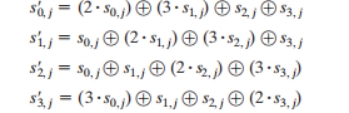
**MixColumns Transformation**

Each byte of a column is mapped into a new value that is a function of all four bytes in that column.



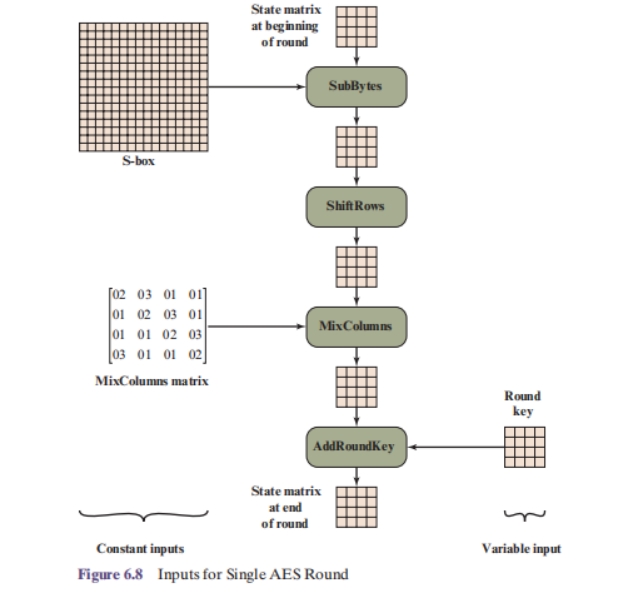
The MixColumns transformation on a single column of **State**

can be expressed as



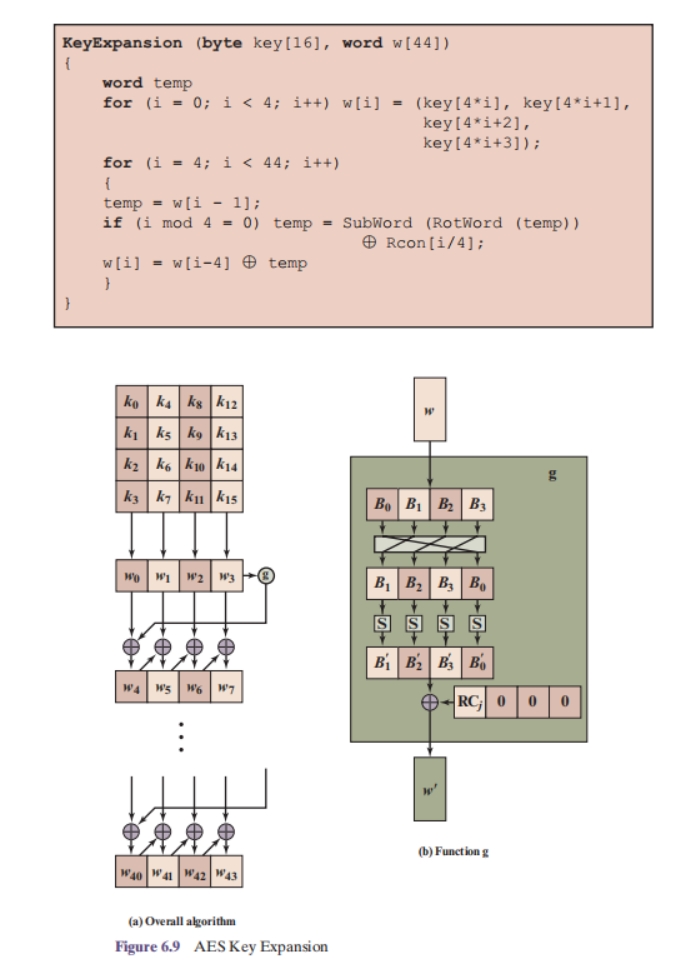
**AddRoundKey Transformation**

In the **forward add round key transformation**, called AddRoundKey, the 128 bits of **State** are bitwise XORed with the 128 bits of the round key shown The operation is viewed as a columnwise operation between the 4 bytes of a **State** column and one word of the round key; it can also be viewed as a byte-level operation.



**Key Expansion Algorithm**

The AES **key expansion** algorithm takes as input a four-word (16-byte) key and produces a linear array of 44 words (176 bytes). This is sufficient to provide a fourword round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher.



**1.** RotWord(Row shift) performs a one-byte circular left shift on a word. This means that an

input word [B0, B1, B2, B3] is transformed into [B1, B2, B3, B0].

**2.** SubWord(S box substitute byte) performs a byte substitution on each byte of its input word, using the

S-box (Table 6.2a).

**3.** The result of steps 1 and 2 is XORed with a round constant, Rcon[j].

The round constant is a word in which the three rightmost bytes are always 0.

Thus, the effect of an XOR of a word with Rcon is to only perform an XOR on the leftmost byte of the word.

