INTRODUCTION TO ENCRYPTION

In This Session:

1. History of cryptography
2. Symmetric-key encryption
3. Public-key encryption
4. Block Ciphers and Stream Ciphers
5. Digital Signatures

Historical Perspective

- Cryptography can be traced back from 4000 years ago used by Egyptians .
- Cryptography was used as a tool to protect national secrets and strategies.
- The proliferation of computers and communications systems in the 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services.
- **DES, the Data Encryption Standard**, is the most well-known cryptographic mechanism in history. It remains the standard means for securing electronic commerce for many financial institutions around the world.
- The most striking development in the history of cryptography came in **1976 when Diffie and Hellman published New Directions in Cryptography.**
- This paper introduced the revolutionary concept of public-key cryptography and also provided a new and ingenious method .
- Although the authors had no practical realization of a **public-key encryp-tion scheme** at the time, the idea was clear and it generated extensive interest and activity in the cryptographic community.
- **In 1978 Rivest, Shamir, and Adlema**n discovered the first practical public-key encryption and signature scheme, now referred to as **RSA.**
- The RSA scheme is based on another hard mathematical problem, the intractability of factoring large integers.
- This application of a hard mathematical problem to cryptography revitalized efforts to find more efficient methods to factor.
- The 1980s saw major advances in this area but none which rendered the RSA system insecure.
- Another class of powerful and practical public-key schemes was found by **ElGamal in 1985**.
- One of the most significant contributions provided by public-key cryptography is the digital

signature.

- In **1991** the first international standard for **digital signatures (ISO/IEC 9796)** was adopted. It is based on the **RSA public-key schem**e.
- **In 1994 the U.S. Government adopted the Digital Signature Standar**d, a mechanism based on the ElGamal public-key scheme.
- The search for new public-key schemes, improvements to existing cryptographic mechanisms, and proofs of security continues at a rapid pace.
- Various standards and infrastructures involving cryptography are being put in place.
- Security products are being developed to address the security needs of an information intensive society.

Definition Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cryptography is not the only means of providing information security, but rather one set of techniques.

Cryptographic Goals

Of all the information security objectives listed below, the following four form a framework upon which the others will be derived:

1. Privacy or confidentiality
2. Data integrity
3. Authentication
4. Non-repudiation

1. **Confidentiality** is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy.
   - There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.
2. **Data integrity** is a service which addresses the unauthorized alteration of data.
   - To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties.
   - Data manipulation includes such things as insertion, deletion, and substitution.
3. **Authentication** is a service related to identification. This function applies to both entities and information itself.
   - Two parties entering into a communication should identify each other.
   - Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc.
   - For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication.
   - Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).
4. **Non-repudiation**
   - When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary.
   - For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted.
   - A procedure involving a trusted third party is needed to resolve the dispute.

Basic Mathematical functions

It is prudent that you be familiarity with basic mathematical concepts . One concept which is absolutely fundamental to cryptography is that of a **function** .

A function is alternately referred to as a mapping or a transformation. We discuss different types of functions that are critical to cryptography.

1-1, one-way and trapdoor one-way Functions

1. A set consists of distinct objects which are called elements of the set.
2. For example, a set X might consist of the elements a, b, c, and this is denoted X = {a, b, c}.

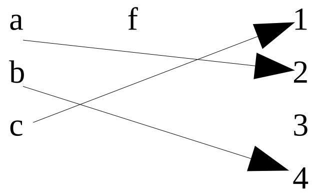
Definition

A function is defined by two sets **X** and **Y** and a rule **f** which assigns to each element in **X** precisely one element in **Y** .

- The set X is called the domain of the function and **Y** the codomain. If **x** is an element of **X** (usually written **x ∈ X**) the image of x is the element in **Y** which the rule **f** associates with **x**; the image y of **x** is denoted by **y = f (x).**
- Standard notation for a function **f** from set **X** to set **Y** is **f : X → Y . If y ∈ Y** , then a
- **preimag**e of **y** is an element **x ∈ X** for which **f (x) = y**.
- The set of all elements in **Y** which have at least one **preimage** is called the **image of f** , denoted **Im(f)**.

Example I

Consider the sets **X = {a, b, c}, Y = {1, 2, 3, 4}**, and the rule **f** from **X** to **Y** defined as **f (a) = 2, f (b) = 4, f (c) = 1.** The figure shows a schematic of the sets **X, Y** and the function **f** . The preimage of the element **2** is **a.** The image of f is **{1, 2, 4}**.



- In the Figure each element in the domain X has precisely one arrowed line originating from it.
- Each element in the codomain Y can have any number of arrowed lines incident to it (including zero lines).

Example II

Take **X = {1, 2, 3, . . . , 10**} and let f be the rule that for each **x ∈ X, f (x) = $\mathbf{r_x}$,** where $\mathbf{r_x}$ is the remainder when $\mathbf{x^2}$ is divided by **11**.

Explicitly then

f (1) = 1 f (2) = 4 f (3) = 9 f (4) = 5 f (5) = 3 f (6) = 3 f (7) = 5 f (8) = 9 f (9) = 4 f (10) = 1.

The image of f is the set **Y = {1, 3, 4, 5, 9}**.

Example III (function)

- Take X = {1, 2, 3, . . . , 10^{50} } and let f be the rule f (x) = r^x , where r_x is the remainder when x^2 is divided by 10^{50} + 1 for all x ∈ X.
- Here it is not feasible to write down **f** explicitly as in the above Example. but nonetheless the function is completely specified by the domain and the mathematical description of the rule f .

I) 1-1 functions

1. **Definition** A function (or transformation) is 1− 1 (one-to-one) if each element in the

codomain Y is the image of at most one element in the domain X. (Only one mapping)

2. **Definition** A function (or transformation) is **onto** if each element in the **codomain Y** is

the image of at least one element in the **domain**.

- Equivalently, a function **f : X → Y** is onto if **Im(f) = Y** .

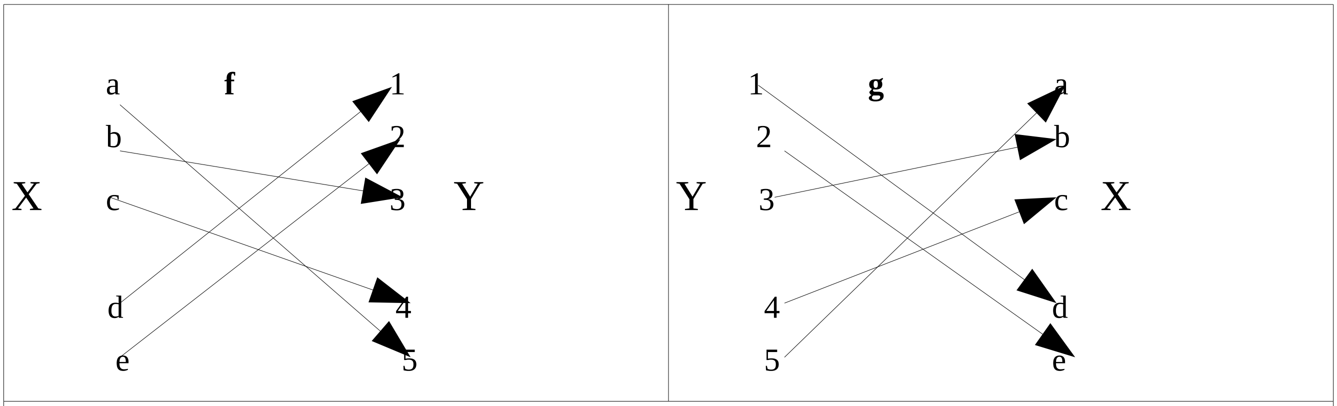
3. **Definition** If a function **f : X → Y** is **1−1** and **Im(f) = Y** , then **f** is called a **bijection**.

- Fact If **f : X → Y** is **1 − 1** then **f : X→ Im(f)** is a **bijection**.
- In particular, if **f : X→ Y** is **1 − 1**, and **X** and **Y** are finite sets of the same size, then f is a **bijection.**
- In terms of the schematic representation, if **f** is a **bijection**, then each element in **Y** has exactly one arrowed line incident with it. The functions described in Examples 1 and 2 are not **bijections.**

In the Example 1 the element 3 is not the image of any element in the domain. In the Example ii each element in the codomain has two preimages.

4. **Definition** If **f** is a **bijection** from X to Y then it is a simple matter to define a bijection g from Y to X as follows: for each y ∈ Y define g(y) = x where x ∈ X and f (x) = y.

   This function **g** obtained from **f** is called the i**nverse function of f** and is denoted by **g = f** $^{\mathbf{-1}}$ **.**



A bijection **f** and its inverse $\mathbf{g = f^{-1}}$.

Example IV (inverse function)

- Let **X = {a, b, c, d, e}**, and **Y = {1, 2, 3, 4, 5}**, and consider the rule f given by the arrowed edges in Figure 1 above. f is a **bijection** and its **inverse g** is formed simply by reversing the arrows on the edges. The domain of **g is Y** and the **codomain is X**.
- Note that if f is a **bijection**, then so is $\mathbf{f^{-1}}$. In cryptography **bijections** are used as the tool for encrypting messages and the inverse transformations are used to **decrypt**. Notice that if the transformations were not **bijections** then it would not be possible to always decrypt to a unique message.

II)One-way functions

There are certain types of functions which play significant roles in cryptography.

1. **Definition** A function **f** from a set **X** to a set **Y** is called a one-way function if **f (x)** is "easy" to compute for all **x ∈ X** but for "essentially all" elements **y ∈ Im(f)** it is "computationally infeasible" to find any **x ∈ X** such that **f (x) = y**.

Note

1. The phrase "for essentially all elements in Y " refers to the fact that there are a few values **y ∈ Y** for which it is easy to find an **x ∈ X** such that **y = f (x)**. For example, one may compute **y = f (x)** for a small number of x values and then for these, the inverse is known by table look-up. An alternate way to describe this property of a one-way function is the following: for a random **y ∈ Im(f)** it is computationally infeasible to find any **x ∈ X** such that **f (x) = y**.

The concept of a one-way function is illustrated through the following examples.

Example V (one-way function) Take **X = {1, 2, 3, . . . , 16}** and define **f (x) =** $\mathbf{r^x}$ for all

x ∈ X where $\mathbf{r^x}$ is the remainder when $\mathbf{3^x}$ is divided by 17. Explicitly,

x :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f (x)	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

- Given a number between 1 and 16, it is relatively easy to find the image of f . However, given a number such as 7, without having the table in front of you, it is harder to find x given that **f (x) = 7**.
- Of course, if the number you are given is **3** then it is clear that **x = 1** is what you need; but for most of the elements in the **codomain** it is not that easy.
- One must keep in mind that this is an example which uses very small numbers; the important point here is that there is a difference in the amount of work to compute f (x) and the amount of work to find x given f (x).
- Even for very large numbers, f (x) can be computed efficiently using the repeated square-and-multiply algorithm whereas the process of finding x from f (x) is much harder.

Example VI(one-way function)

- A prime number is a positive integer greater than 1 whose only positive integer divisors are 1 and itself.
- Select primes **p = 48611**, and **q = 53993**, form **n = pq = 2624653723**, and let **X = {1, 2, 3, . . . , n − 1}.**
- Define a function **f** on **X** by **f (x) = r_x** for each x ∈ X, where r_x is the remainder when x^3 is divided by n.
- For instance, f(2489991) = 1981394214 since 2489991^3 = 5881949859.n + 1981394214.
- Computing f (x) is a relatively simple thing to do, but to reverse the procedure is much more difficult; that is, given a remainder to find the value x which was originally cubed (raised to the third power).
- This procedure is referred to as the **computation of a modular cube root with modulus n**.
- If the factors of n are unknown and large, this is a difficult problem; however, if the factors p and q of n are known then there is an efficient algorithm for computing modular cube roots.

II) Trapdoor one-way functions

Definition A trapdoor one-way function is a one-way function **f : X→ Y** with the additional property that given some extra information (called the **trapdoor information**) it becomes feasible to find for any given **y ∈ Im(f)**, an **x ∈ X** such that **f (x) = y**.

Example VII illustrates the concept of a trapdoor one-way function.

- With the additional information of the factors of **n = 2624653723** (namely, **p = 48611** and **q = 53993**, each of which is five decimal digits long) it becomes much easier to invert the function.
- The factors of 2624653723 are large enough that finding them by hand computation would be difficult.
- Of course, any reasonable computer program could find the factors relatively quickly.
- If, on the other hand, one selects **p** and **q** to be very large distinct prime numbers (each having about 100 decimal digits) then, by today's standards, it is a difficult problem, even with the most powerful computers, to deduce **p** and **q** simply from **n**.
- This is the well known integer factorization problem and a source of many trapdoor one-way functions.
- The trap door information here is the fact that **p** and **q** are prime numbers
- It remains to be rigorously established whether there actually are any (true) one-way functions.
- That is to say, no one has yet definitively proved the existence of such functions under reasonable (and rigorous) definitions of "**easy**" and "computationally infeasible".
- Since the existence of one-way functions is still unknown, the existence of trapdoor one-way functions is also unknown.
- However, there are a number of good candidates for one-way and trapdoor one-way functions.
- One-way and trapdoor one-way functions are the basis for public-key cryptography

Permutations

- Permutations are functions which are often used in various cryptographic constructs.

Definition Let **S** be a finite set of elements. A permutation **p** on **S** is a bijection from S to itself (i.e., **p : S** → S).

Example (permutation) Let **S = {1, 2, 3, 4, 5}**. A permutation **p : S** → **S** is defined as follows:

p(1) = 3, p(2) = 5, p(3) = 4, p(4) = 2, p(5) = 1.

- A permutation can be described in various ways. It can be displayed as below

$$p=\begin{pmatrix}1\,2\,3\,4\,5\\3\,5\,4\,2\,1\end{pmatrix}$$

where the top row in the array is the domain and the bottom row is the image under the mapping **p**.

- Since permutations are bijections, they have inverses.
- If a permutation is written as an array. Its inverse is easily found by:

1. Interchanging the rows in the array and
2. Reordering the elements in the new top row if desired (the bottom row would have to be reordered correspondingly).

The inverse of p in is $p^{-1}=\begin{pmatrix}1\,2\,3\,4\,5\\5\,4\,1\,3\,2\end{pmatrix}$

Example (permutation)

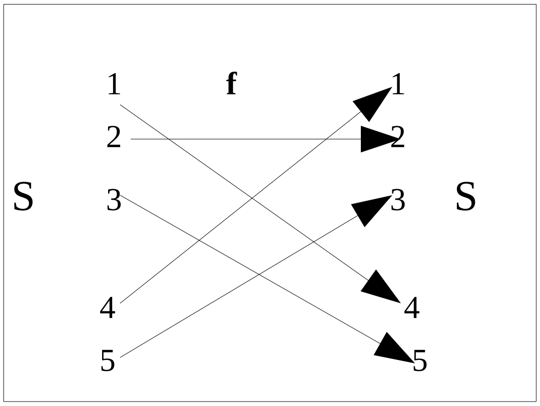
- Let X be the set of integers **{0, 1, 2, . . . , pq − 1}** where **p** and **q** are distinct large primes (for example, **p** and **q** are each about 100 decimal digits long), and suppose that neither **p−1** nor q **−1** is divisible by 3. Then the function $\mathbf{p(x) = r_x}$, where $\mathbf{r_x}$ is the remainder when x^3 is divided by pq, can be shown to be a permutation.
- Determining the inverse permutation is computationally infeasible by today's standards unless p and q are known

Involutions

- Involutions are functions that have the property that they are their own inverses.
- **Definition** Let S be a finite set and let **f** be a bijection from S to S (i.e., f : S → S).
- The function **f** is called an involution if **$f = f^{-1}$** . An equivalent way of stating this is **$f(f(x)) = x$ for all $x \in S$.**

Example (involution)

- Figure is an example of an involution. In the diagram of an involution, note that if j is the image of i then i is the image of j.



Some Basic terminology and concepts

Encryption domains and codomains Symbols

- **A** denotes a finite set called the alphabet of definition. For example, A = {0, 1}, the binary alphabet, is a frequently used alphabet of definition. Note that any alphabet can be encoded in terms of the binary alphabet. For example, since there are 32 binary strings of length five, each letter of the English alphabet can be assigned a unique binary string of length five.
- **M** denotes a set called the message space. M consists of strings of symbols from an alphabet of definition.
  - An element of M is called a plaintext message or simply a plaintext.
  - For example, M may consist of binary strings, English text, computer code, etc.
- **C** denotes a set called the ciphertext space. **C** consists of strings of symbols from an alphabet of definition, which may differ from the alphabet of definition for M.
  - An element of C is called a ciphertext.

Encryption and decryption transformations Symbols

- **K** denotes a set called the key space. An element of **K** is called a key.
- Each element **e ∈ K** uniquely determines a bijection from **M** to **C**, denoted by **E_e** . **Ee** is called an encryption function or an encryption transformation.
- Note that **E_e** must be a bijection if the process is to be reversed and a unique plaintext message recovered for each distinct ciphertext. 1
- For each **d ∈ K**, **D_d** denotes a bijection from **C to M** (i.e., **D d : C** → **M**). **D_d** is called a decryption function or decryption transformation.
- The process of applying the transformation **E_e** to a message **m ∈ M** is usually referred to as encrypting m or the encryption of m.
- The process of applying the transformation **D_d** to a ciphertext c is usually referred to as decrypting c or the decryption of c.
- An encryption scheme consists of a set {**Ee : e ∈ K**} of encryption transformations and a corresponding set {**Dd : d ∈ K**} of decryption transformations with the property that for each **e ∈ K** there is a unique key d ∈ K such that **D d = Ee** ; that is, **Dd (Ee (m)) = m** for all **m ∈** M. An encryption scheme is sometimes referred to as a cipher.
- The keys **e** and **d** in the preceding definition are referred to as a key pair and sometimes denoted by **(e, d).** Note that e and d could be the same.
- To construct an encryption scheme requires one to select a message space M, a ciphertext space C, a key space K, a set of encryption transformations **{E e : e ∈ K},** and a corresponding set of decryption transformations **{D d : d ∈ K}**.

Achieving Confidentiality

An encryption can be used to achieving confidentiality.

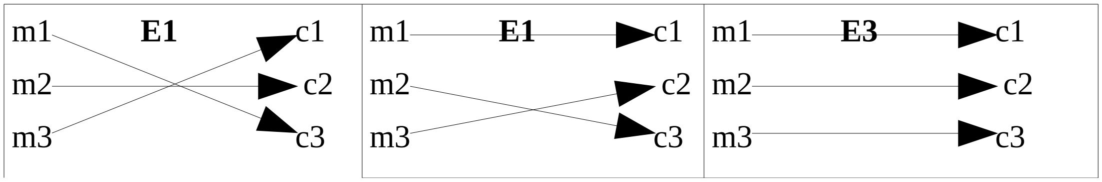
- Two parties **Alice** and **Bob** first secretly choose or **secretly exchange a key pair (e, d)**.
- At a subsequent point in time, if **Alice** wishes to send a message **m ∈ M** to **Bob**,
    - She computes **c = Ee (m)** (**Encrypt**) and transmits this to **Bob**.
    - Upon receiving **c**, **Bob** computes **D d (c) = m** (**dycrypt**)and hence recovers the original message m.
- **Why use keys.**
- Why not just choose one **encryption function** and its corresponding **decryption function**?
- *Having transformations which are very similar but characterized by keys means that if some particular **encryption/decryption transformation** is revealed then one does not have to redesign the entire scheme but simply change the key.*
- It is sound cryptographic practice to change the key (encryption/decryption transformation) frequently.

Example Illustration

1. As an example, consider an ordinary resettable combination l**ock/padlock/SwitchCase** lock. The structure of the lock is available to anyone who wishes to purchase one but the combination is chosen and set by the owner.
2. If the owner suspects that the combination has been revealed he can easily reset it without replacing the physical mechanism.

Example (encryption scheme)

- Let **M = {m1 , m2 , m3 }** and **C = {c1 , c2 , c3 }**. There are precisely **3! = 6 bijections** from M to **C**.
- The **key space K = {1, 2, 3, 4, 5, 6}** has six elements in it, each specifying one of the transformations. We illustrates three of the six encryption functions which are denoted by **E i , 1 ≤ i ≤ 6.**
- **Alice** and **Bob** agree on a transformation, say **E1** . To encrypt the message **m1** , Alice computes **E1 (m1) = c3** and sends **c3** to **Bob**.
- **Bob** decrypts **c3** by reversing the arrows on the diagram for **E 1** and observing that **c3** points to m1 .



Security

- A fundamental premise in cryptography is that the sets **M, C, K, {Ee : e ∈ K}, {Dd : d ∈ K}** are **public knowledg**e.
- When two parties wish to communicate securely using an encryption scheme, the only thing that they keep secret is the particular key pair **(e, d)** which they are using, and which they must select.
- One can gain additional security by keeping the class of encryption and decryption transformations secret but one should not base the security of the entire scheme on this approach.

Definitions

1. An encryption scheme is said to be **breakable** if a third party, without prior knowledge of the key pair **(e, d)**, can systematically recover plaintext from corresponding ciphertext within some appropriate time frame.
    - *An appropriate time frame will be a function of the useful lifespan of the data being protected.*
    - **For example**, an instruction to buy a certain stock may only need to be kept secret for a few minutes whereas state secrets may need to remain confidential indefinitely.
    - An encryption scheme can be broken by trying all possible keys to see which one the communicating parties are using (assuming that the class of encryption functions is public knowledge).
    - This is called an **exhaustive search** of the key space.
    - This means that the number of keys (i.e.the size of the key space) should be large enough to make this approach computationally infeasible.
    - It is the objective of a designer of an encryption scheme that this be the best approach to break the system.

Requirements for a good Security Encryption System

A good cipher scheme is that

1. The system should be, if not theoretically unbreakable, unbreakable in practice;

2. Compromise of the system details should not inconvenience the correspondents;

3. The key should be rememberable without notes and easily changed;

4. The cryptogram should be transmissible by telegraph;

5. The encryption apparatus should be portable and operable by a single person; and

6. The system should be easy, requiring neither the knowledge of a long list of rules nor

mental strain.

More Definitions

- **Cryptanalysis** is the study of mathematical techniques for attempting to defeat cryptographic techniques, and, more generally, information security services.
- **A cryptanalyst** is someone who engages in cryptanalysis.
- **Cryptology** is the study of cryptography and cryptanalysis.
- **A cryptosystem** is a general term referring to a set of cryptographic primitives used to provide information security services. M

Types of Cryptography

Cryptographic techniques are typically divided into two generic types:

1. symmetric-key Cryptography
2. and public-key Cryptography .

Symmetric-key encryption

Definition

Consider an encryption scheme consisting of the sets of encryption and decryption transformations **{Ee : e ∈ K}** and **{Dd : d ∈ K}**, respectively, where **K** is the key space.

- The encryption scheme is said to be **symmetric-key** if for each associated encryption/decryption key pair **(e, d)**, it is computationally "**easy**" to determine **d** knowing only **e**, and to determine **e** from **d**.
- Since **e = d** in most practical symmetric-key encryption schemes, the term symmetric key becomes appropriate.

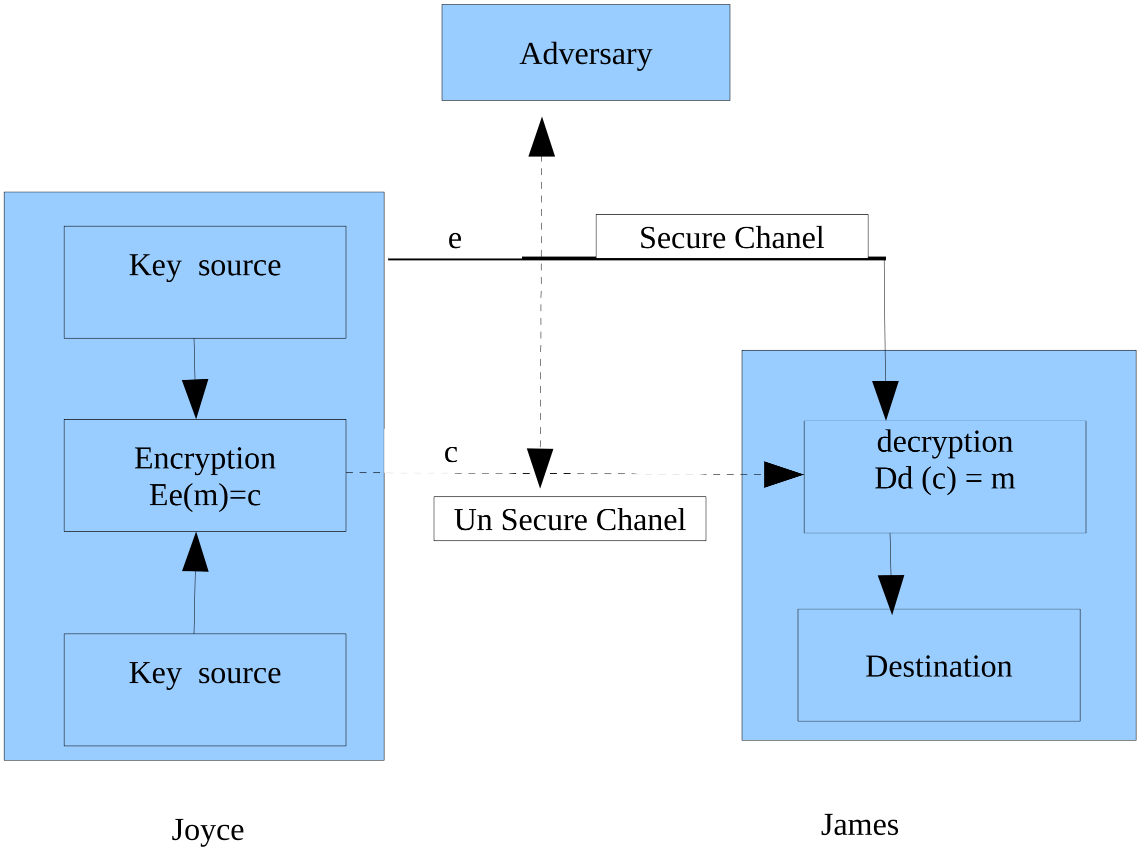
Example 1 to illustrates the idea of symmetric-key encryption.

- Let **A = {A, B, C, . . . , X, Y, Z**} be the English alphabet.
- Let **M** and **C** be the set of all strings of length five over A. The key **e** is chosen to be a permutation on **A**.
- To encrypt, an English message is broken up into groups each having five letters (with appropriate padding if the length of the message is not a multiple of five) and a permutation e is applied to each letter one at a time.
- To decrypt, the inverse permutation **d = e**$^{-1}$ is applied to each letter of the ciphertext.
- For instance, suppose that the key **e** is chosen to be the permutation which maps each letter to the one which is three positions to its right, as shown below

$$e=\begin{pmatrix} A\,B\,C\,D\,E\,F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S\,T\,U\,V\,W\,X\,Y\,Z \\ D\,E\,F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S\,T\,U\,V\,W\,X\,Y\,Z\,A\,B\,C \end{pmatrix}$$

The message m = THISC IPHER ISCER TAINL YNOTS ECURE is encrypted to

c = Ee (m) = WKLVF LSKHU LVFHU WDLQO BQRWV HFXUH.



- One of the major issues with symmetric-key systems is to find an efficient method to agree upon and exchange keys securely.
- This problem is referred to as the **key distribution problem**.
- It is assumed that all parties know the set of encryption/decryptiontransformations (i.e., they all know the encryption scheme).
- Remember that the only information which should be required to be kept secret is the key **B**.
- However, in symmetric-key encryption, this means that the key **e** must also be kept secret, as **d** can be deduced from e. In the figure above the encryption key **e** is transported from one entity to the other with the understanding that both can construct the **decryption key d**.

There are two classes of symmetric-key encryption schemes which are commonly distinguished:

1. block ciphers and
2. stream ciphers.

block ciphers

Definition

A block cipher is an encryption scheme which breaks up the plaintext messages to be transmitted into strings (called blocks) of a fixed length **t** over an alphabet **A**, and encrypts one block at a time.

Most well-known symmetric-key encryption techniques are block ciphers.

Classes of block ciphers are :

1. Substitution ciphers and
2. Transposition ciphers
3. Product ciphers is combine os these two

Substitution ciphers and transposition ciphers

Substitution ciphers are block ciphers which replace symbols (or groups of symbols) by other symbols or groups of symbols.

Simple Substitution Cipher

Definition

Let **A** be an alphabet of **q** symbols and **M** be the set of all strings of length **t** over **A**. Let **K** be the set of all permutations on the set **A**.

- Define for each **e ∈ K** an encryption transformation **Ee** as follows:
- **Ee (m) = (e(m1)e(m2) · · · e(mt)) = (c1 c2 · · · ct) = c,** where **m = (m1 m2 · · · mt) ∈ M**.
- In other words, for each symbol , replace (substitute) it by another symbol from **A** according to some fixed permutation e.
- To decrypt **c = (c1 c2 · · · ct)** compute the inverse permutation **d = e** $^{-1}$ and **Dd (c) = (d(c1)d(c2) · · · d(ct)) = (m1 m2 · · · mt) = m.**
- **Ee** is called a **simple substitution cipher** or a **mono-alphabetic substitution cipher**.

Note

1. The number of distinct substitution ciphers is **q!** and is independent of the block size in the cipher. *The Example I above is an example of a simple substitution cipher of block length five.*
2. Simple substitution ciphers over small block sizes provide inadequate security even when the key space is extremely large.
3. If the alphabet is the English alphabet as in Example 1 then the size of the key space is **26! ≈ 4 × 10 26 ,** yet the key being used can be determined quite easily by examining a modest amount of **ciphertext**.
4. This follows from the simple observation that the distribution of letter frequencies is preserved in the **ciphertext.**

5. For example, the letter E occurs more frequently than the other letters in ordinary English text. Hence the letter occurring most frequently in a sequence of **ciphertext** blocks is most likely to correspond to the letter E in the **plaintext.**
6. By observing a modest quantity of **ciphertext** blocks, a **cryptanalyst** can determine the key.

Homophonic Substitution Ciphers

Definition To each symbol **a ∈ A**, associate a set **H(a)** of strings of **t** symbols, with the restriction that the sets **H(a)**, **a ∈ A**, be pairwise disjoint.

- A **homophonic substitution** cipher replaces each symbol a in a **plaintext** message block with a **randomly chosen** string from **H(a)**.
- To **decrypt** a string **c** of **t** symbols, one must determine an **a ∈ A** such that **c ∈ H(a)**.
- The key for the cipher consists of the sets **H(a)**.

Example II (homophonic substitution cipher)

Consider **A = {a, b}, H(a) = {00, 10},** and **H(b) = {01, 11}.** The plaintext message block **ab** encrypts to one of the following: **0001, 0011, 1001, 1011.**

Note that the codomain of the encryption function (for messages of length two) consists of the following pairwise disjoint sets of 4-element bitstrings:

aa → **{0000, 0010, 1000, 1010}**

ab → **{0001, 0011, 1001, 1011}**

ba → **{0100, 0110, 1100, 1110}**

bb → **{0101, 0111, 1101, 1111}**

- Any 4-bitstring uniquely identifies a codomain element, and hence a plaintext message
- Often the symbols do not occur with equal frequency in plaintext messages.
- With a simple substitution cipher this non-uniform frequency property is reflected in the ciphertext as illustrated in ExampleI.
- A homophonic cipher can be used to make the frequency of occurrence of ciphertext symbols more uniform, at the expense of data expansion.
- Decryption is not as easily performed as it is for simple substitution ciphers.

Polyalphabetic Substitution ciphers

Definition A polyalphabetic substitution cipher is a block cipher with block length **t** over an alphabet **A** having the following properties:

1. The key space **K** consists of all ordered sets of **t** permutations **(p1 , p2 , . . . , pt)**, where each permutation **pi** is defined on the set **A**;
2. Encryption of the message **m = (m1 m2 · · · mt)** under the **key e = (p1 , p2 , . . . , pt)** is given by **Ee (m) = (p1 (m1)p2 (m2) · · · pt (mt))**; and
3. The decryption key associated with **e = (p1 , p2 , . . . , pt)** is **d =** (p^{-1} , p^{-1} , . . . , p^{-1})**.**

Example

Let **A = {A, B, C, . . . , X, Y, Z**} and **t = 3**. Choose **e = e (p1 , p2 , p3)**, where **p1** maps each letter to the letter three positions to its right in the alphabet, **p2** to the one seven positions to its right, and **p3** ten positions to its right.

If **m = THI SCI PHE RIS CER TAI NLY NOT SEC URE**

then

c = Ee (m) = WOS VJS SOO UPC FLB WHS QSI QVD VLM XYO.

- Polyalphabetic ciphers have the advantage over simple substitution ciphers that symbol frequencies are not preserved.
- In the example above, the letter **E** is encrypted to both **O** and **L.**
- However, polyalphabetic ciphers are not significantly more difficult to cryptanalyze, the approach being similar to the simple substitution cipher.
- In fact, once the block length **t** is determined, the ciphertext letters can be divided into **t** groups (where group **i, 1 ≤ i ≤ t,** consists of those ciphertext letters derived using permutation **p i**), and a frequency analysis can be done on each group.

Transposition ciphers

Transposition cipher, which simply permutes the symbols in a block.

Definition

Consider a symmetric-key block encryption scheme with block length **t**. Let **K** be the set of all permutations on the set **{1, 2, . . . , t}**.

For each **e ∈ K** define the encryption function **Ee (m) = (me(1) me(2) · · · me(t))** where **m = (m1 m2 · · · mt) ∈ M,** the message space.

- The set of all such transformations is called a simple transposition cipher.
- The decryption key corresponding to **e** is the inverse permutation **d =** e^{-1} . To decrypt **c = (c1 c2 · · · ct),** compute **Dd (c) = (cd(1) cd(2) · · · cd(t))**.
- A simple transposition cipher preserves the number of symbols of a given type within a block, and thus is easily **cryptanalyzed**.

Example of Transposition Cipher......................

Composition of ciphers

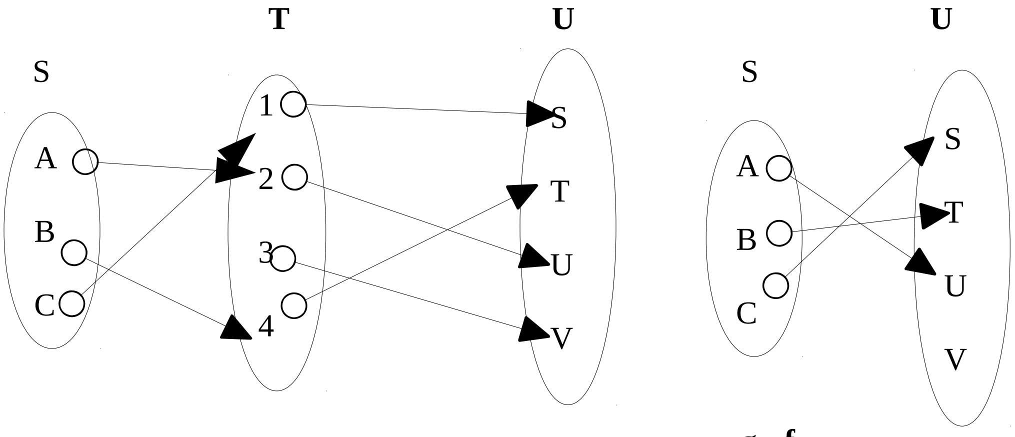
In order to describe product ciphers, the concept of composition of functions is introduced. Compositions are a convenient way of constructing more complicated functions from simpler ones.

Composition of functions

Definition

Let **S, T** , and **U** be finite sets and let f : **S −→ T** and **g : T −→ U** be functions.

The composition of **g** with **f** , denoted **g ◦ f** (or simply **gf**), is a function from S to U as illustrated in the Figure below and defined by **(g ◦ f)(x)** = **g(f (x))** for all **x ∈ S**.



g ◦ f

Note

- Composition can be easily extended to more than two functions.
- For functions f 1 , f2 , . . . , ft , one can define ft ◦ · · ·◦ f2 ◦ f1 , provided that the domain of f_t equals the codomain of f_{t-1} and so on.

Product ciphers

- Simple substitution and transposition ciphers individually do not provide a very high level of security. However, by combining these transformations it is possible to obtain strong ciphers.
- Some of the most practical and effective symmetric-key systems are product ciphers.
- One example of a product cipher is a composition of $t \geq 2$ transformations **Ek1 Ek2 · · · Ek**t where each **Eki , 1 ≤ i ≤ t,** is either a substitution or a transposition cipher.
- For the purpose of this introduction, let the composition of a substitution and a transposition be called a round.

Example (product cipher)

Let M = C = K be the set of all binary strings of length 6.

The number of elements in **M** is $2^6 = 64$. **Let m = (m1 m2 · · · m6)** and define

$E_k^{(1)}(m) = m \oplus k$, where $k \in K$,

$E^{(2)}(m) = (m_4\ m_5\ m_6\ m_1\ m_2\ m_3)$.

- Here, ⊕ is the **exclusive-OR (XOR)** operation defined as follows:

  $0 \oplus 0 = 0,\ 0 \oplus 1 = 1,\ 1 \oplus 0 = 1,\ 1 \oplus 1 = 0.$
- $E_k^{(1)}$is a polyalphabetic substitution cipher and $E^{(2)}$ is a transposition cipher (not involving the key). The product $E_k^{(1)} E^{(2)}$ is a round.
- While here the transposition cipher is very simple and is not determined by the key, this need not be the case.

NOTE: (**confusion and diffusion**)

- A substitution in a round is said to add confusion to the encryption process whereas a transposition is said to add diffusion.
- Confusion is intended to make the relationship between the key and ciphertext as complex as possible.
- Diffusion refers to rearranging or spreading out the bits in the message so that any redundancy in the plaintext is spread out over the ciphertext.
- A round then can be said to add both confusion and diffusion to the encryption.
- Most modern block cipher systems apply a number of rounds in succession to encrypt plaintext.

Stream ciphers

- Stream ciphers very simple block ciphers having block length equal to **1**.
- What makes them useful is the fact that the encryption transformation can change for each symbol of plaintext being encrypted. That is the transformation changes with time.
- In situations where transmission errors are highly probable, stream ciphers are advantageous because they have no error propagation.
- They can also be used when the data must be processed one symbol at a time (e.g., if the equipment has no memory or buffering of data is limited).

Definition

Let **K** be the key space for a set of encryption transformations. A sequence of symbols **e1 e2 e3 · · · ei ∈ K,** is called a keystream.

Definition

Let **A** be an alphabet of **q** symbols and let $\mathbf{E_e}$ be a simple substitution cipher with block length **1** where **e ∈ K**. Let **m1 m2 m3 · · ·** be a plaintext string and let **e1 e2 e3 · · ·** be a keystream from **K**.

A stream cipher takes the plaintext string and produces a ciphertext string **c1 c2 c3 · · ·** where **ci = Eei (mi)**. If **di** denotes the inverse of **ei** ,then $\mathbf{D_{di}}$ **(ci) = mi** decrypts the ciphertext string.

- A stream cipher applies simple encryption transformations according to the keystream being used.
- The keystream could be generated at random, or by an algorithm which generates the keystream from an initial small keystream (called a seed), or from a seed and previous ciphertext symbols.
- Such an algorithm is called a keystream generator.

There are many stream ciphers each with its own definition of keystream generator.

Examples of stream ciphers include:

1. the Vernam cipher,
2. Rivest cipher , and
3. The one-time pads

The Vernam Stream cipher

Definition

The Vernam Cipher is a stream cipher defined on the alphabet **A = {0, 1}**. A binary message $\mathbf{m_1\ m_2 \cdots m_t}$ is operated on by a **binary key** string $\mathbf{k_1 k_2 \cdots k_t}$ of the same length to produce a ciphertext string **c 1 c2 · · ·** ct where **ci = mi ⊕ ki , where 1 ≤ i ≤ t.**

If the key string is randomly chosen and never used again, the Vernam cipher is called a **one-time system or a one-time pad**.

You observe that there are precisely two substitution ciphers on the set **A**.

- One is simply the identity map $\mathbf{E_0}$ which sends 0 to 0 and 1 to 1; the other E_1 sends 0 to 1 and 1 to 0.
- If the key string is reused there are ways to attack the system.
- For example, if $\mathbf{c_1\ c_2 \cdots c_t}$ and $\mathbf{c_1'\ c_2' \cdots c_t'}$ are two ciphertext strings produced by the same keystream $k_1\ k_2 \cdots k_t$ then $c_i = m_i \oplus k_i$, $c'_i = m_{i`} \oplus k_i$ and ci ⊕ $c_i$` = $m_i \oplus m_i$` .

Example.

if m=1100 and key space 1010 then

	Binary Plaintext m	**1**	**1**	**0**	**0**	If the keystream contains a 0, apply $\mathbf{E_0}$ to the corresponding plaintext symbol;
	$\mathbf{m_i \oplus k_i}$	**XOR**				
	Binary Key space	1	0	1	0	If the keystream contains a 1, apply $\mathbf{E_1}$ to the corresponding plaintext symbol;
	Cipher text (C)	**0**	**1**	**1**	**0**	
	Binary Plaintext m'	**1**	**0**	**0**	**1**	
	$\mathbf{m'_i \oplus k_i}$	**XOR**				**Reusing the key**
	Binary Key space	1	0	1	0	
	Cipher text (C')	**0**	**1**	**1**	**1**	
	$\mathbf{c'_i \oplus c_i}$	**XOR**				
	Cipher text (C)	**0**	**1**	**1**	**0**	
		0	**0**	**0**	**1**	**ci ⊕** $\mathbf{c_i}$**` =** $\mathbf{m_i \oplus m_i}$**` .**
	$\mathbf{m_i \oplus m'_i}$	**0**	**0**	**0**	**1**	

The redundancy in the latter may permit cryptanalysis.

- The one-time pad can be shown to be **theoretically unbreakable.**
- That is, if a cryptanalyst has a ciphertext string $\mathbf{c}_1 \mathbf{c}_2 \cdots \mathbf{c}_t$ encrypted using a random key string which has been used only once, the cryptanalyst can do no better than guess at the plaintext being any binary string of length t (i.e., **t-bit** binary strings are equally likely as plaintext).
- Notably to realize an unbreakable system requires a random key of the same length as the message.

NOTE

- For some time the communication line between Moscow and Washington was secured by a one-time pad.
- Transport of the key was done by trusted courier.

Note : The key space

- The size of the key space is the number of encryption/decryption key pairs that are available in the cipher system.
- Each can be simply described by a permutation which is called the key.
- One should not be temptated to relate the security of the encryption scheme to the size of the key space. The following statement is important to remember.

A necessary, but usually not sufficient, condition for an encryption scheme to be secure is that the key space be large enough to preclude exhaustive search.

Weaknesses of Stream Ciphers

Stream ciphers have several weaknesses.

1. The most crucial shortcoming of stream ciphers is the fact that patterns in the plaintext can be reflected in the ciphertext. In addition:
   - certain words in the English language appear with predictable regularity.
   - Letters of the alphabet also appear in predictable regularity. e.g.
     - The most commonly used letters of the alphabet in the English language are E, T, A, O, N, and I.
     - The least commonly used letters in the English language are J, K, X, Q, and Z.
     - The most common combination of letters in the English language is "th." As a result, if a code breaker is able to find a "t" in a code, it doesn't take long to find an "h."
2. Another weakness of stream ciphers is that they can be susceptible to a substitution attack even without breaking the code.
     - This is a type of **replay attack** where someone can simply copy a section of an old message and insert it into a new message.

    - You don't need to break the code to insert the old section into a new message.

Examples of widely deployed symmetric key cryptosystems include :

1. DES,
2. IDEA,
3. Blowfish,
4. RC4,
5. CAST, and
6. SKIPJACK.

Digital signatures

Digital signature is a cryptographic means of providing authentication, authorization, and non-repudiation.

The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information.

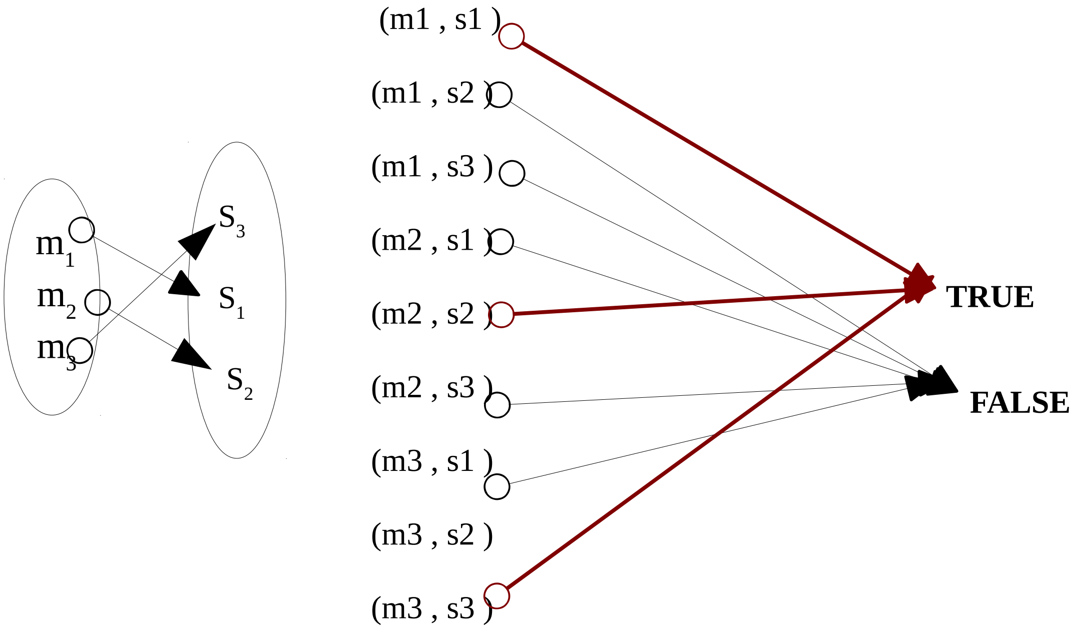
The process of signing entails transforming the message and some secret information held by the entity into a tag called a signature.

Let :

- **M** is the set of messages which can be signed.
- **S** is a set of elements called signatures, possibly binary strings of a fixed length.
- **SA** is a transformation from the message set **M** to the signature set **S**, and is called a signing transformation for entity **A(Alice)**.
- The transformation **SA** is kept secret by **A**, and will be used to create signatures for messages from **M**.
- **VA** is a transformation from the set **M** × **S** to the set **{true, false}**.
- **VA** is called a verification transformation for **A's** signatures, is **publicly known**, and is used by other entities to verify signatures created by **A**.
- *The transformations **SA** and **VA** provide a digital signature scheme for **A***

Illustrating Example (digital signature scheme)

M = {m1 , m2 , m3 } and **S = {s1 , s2 , s3 }.** The diagram below displays a signing function **S A** from the set **M** and, the right side, the corresponding verification function **V A** .



A signing and verification function for a digital signature scheme. s is a valid signature of A on message m if and only if V A (m, s) = true.

It is computationally infeasible for any entity other than A to find, for any m ∈ M, an s ∈ S such that VA (m, s) = true.

The Signing procedure

Entity **A** (the signer) creates a signature for a message **m ∈ M** by doing the following:

1. Compute **s** = **SA (m)**.

2. Transmit the pair **(m, s)**. **s** is called the signature for message **m**.

Verification procedure

To verify that a signature **s** on a message **m** was created by **A**, an entity **B**(Bob) (**the verifier**)

performs the following steps:

1. Obtain the verification function **VA** of **A**.

2. Compute **u = VA (m, s)**.

3. Accept the signature as having been created by **A** if **u = true**, and reject the signature if **u = false**.

NOTE

- The signing algorithm **S A** of **A** is determined by a key **kA** and **A** is only required to keep **k A** secret.
- Similarly, the verification algorithm **VA** of **A** is determined by a key **l A** which is made public.
- On main difference with physical signature is that digital signature is message-dependent.

Properties required for signing and verification functions

There are several properties which the signing and verification transformations must satisfy.

1. s is a valid signature of A on message m if and only if V A (m, s) = true.
2. It is computationally infeasible for any entity other than A to find, for any m ∈ M, an s ∈ S such that VA (m, s) = true.

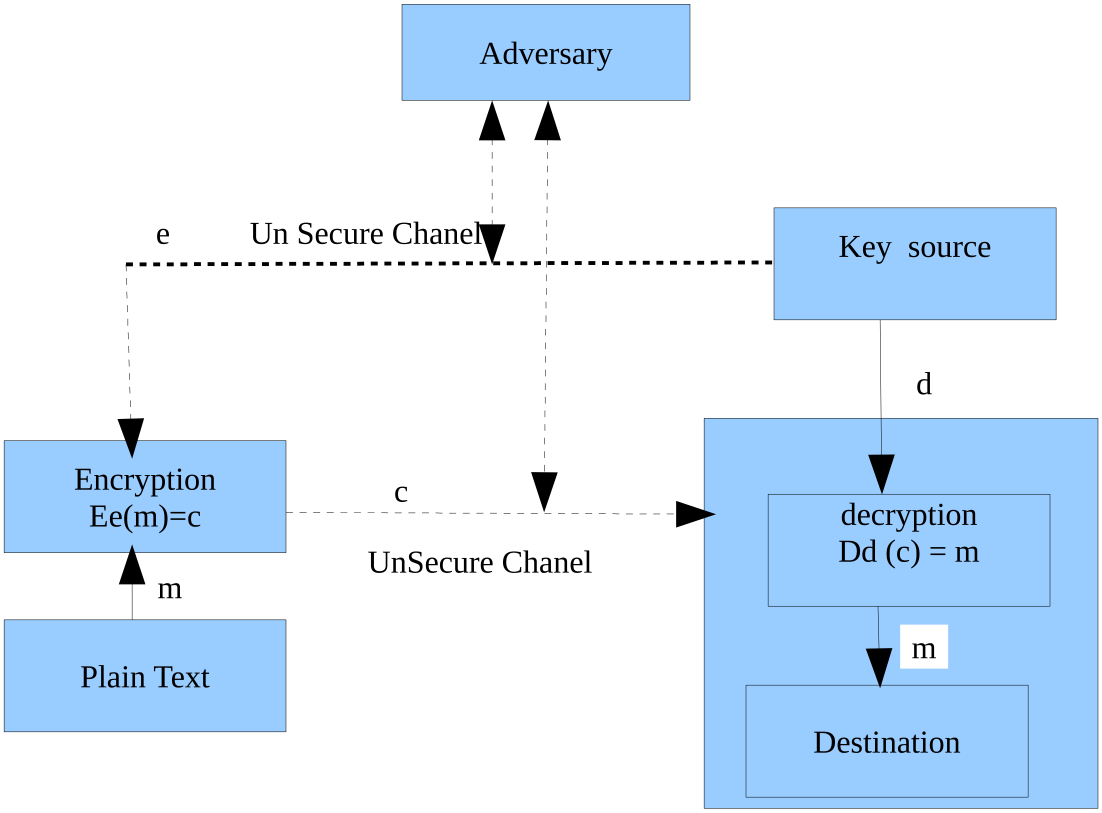
Public-key cryptography

Let **{Ee : e ∈ K}** be a set of encryption transformations, and let **{D d : d ∈ K}** be the set of corresponding decryption transformations, where **K** is the key space.

- Consider any pair of associated encryption/decryption transformations **(E e , Dd)** and suppose that each pair has the property that knowing **E e** it is computationally infeasible, given a random ciphertext
- **c ∈ C**, to find the message **m ∈ M** such that **Ee (m) = c**.
- This property implies that given **e** it is infeasible to determine the corresponding decryption key **d**.
- **Ee** is being viewed here as a **trapdoor one-way function** with **d** being the trapdoor
- information necessary to compute the inverse function and hence allow decryption.
- This is unlike symmetric-key ciphers where **e** and **d** are essentially the same.

Illustrating Example

- Consider a communication between **Alice** and **Bob**
- Bob selects the key pair (e, d). Bob sends the en



- Bob selects the key pair **(e, d)**.
- Bob sends the encryption key **e** (called the **public key**) to Alice over any channel but keeps the decryption key d (called the **private key**) secure and secret.
- Alice may subsequently send a message m to Bob by applying the encryption transformation determined by Bob’s public key to get **c = E e (m)**.
- Bob decrypts the ciphertext **c** by applying the inverse transformation **Dd** uniquely determined by **d**.
- The encryption key is transmitted to Alice over an unsecured channel. This unsecured channel may be the same channel on which the ciphertext is being transmitted .
- Public-key encryption, as described here, assumes that knowledge of the public key e does not allow computation of the private key d.
- In other words, this assumes the existence of trapdoor one-way functions
- **For the scheme to be secure, it must be computationally infeasible to compute d from e.**

The necessity of authentication in public-key systems

- The public-key cryptography scheme outlined above does not requiring a secure channel to pass the encryption key.
- This would imply that two entities could communicate over an unsecured channel without ever having met to exchange keys.
- Unfortunately, this is not . An active adversary can defeat the system (decrypt messages intended for a second entity) without breaking the encryption system by impersonating.
- In this scenario the adversary impersonates entity **B** by sending entity **A** a public key **e** which **A** assumes (incorrectly) to be the public key of **B**.
- The adversary intercepts encrypted messages from **A** to **B**, decrypts with its own private key **d** , **re-encrypts** the message under **B**’s public key **e**, and sends it on to **B**.
- This highlights the necessity to authenticate public keys to achieve data origin authentication of the public keys themselves.
- **A** must be convinced that she is encrypting under the legitimate public key of **B**.

Digital signatures from reversible public-key encryption

Digital signature schemes can also be based on public-key encryption systems.

Suppose **Ee** is a public-key encryption transformation with message space **M** and ciphertext space C. Suppose further that **M = C**.

If **Dd** is the decryption transformation corresponding to **Ee** then since **Ee** and **Dd** are both permutations, one has **Dd (Ee (m)) = Ee (Dd (m)) = m**, for all **m ∈ M**.

A public-key encryption scheme of this type is called reversible.

Note that it is essential that **M = C** for this to be a valid equality for all **m ∈ M**; otherwise, **Dd (m)** will be meaningless for **m ∉ C**.

Construction for a digital signature scheme

1. Let **M** be the message space for the signature scheme.

2. Let **C** = M be the signature space S.

3. Let **(e, d)** be a key pair for the public-key encryption scheme.

4. Define the signing function SA to be Dd . That is, the signature for a message **m ∈ M** is **s = Dd (m)**.

5. Define the verification function VA by

$$\text{VA (m, s)} = \begin{cases} \textbf{true}, \text{ if } \textbf{Ee (s) = m}, \\ \textbf{false}, \text{ otherwise.} \end{cases}$$

Examples of public key algorithms

1. Diffie-Hellman;
2. RSA; and the
3. Digital Signature Algoriths is a valid signature of A on message m if and only if V A (m, s) = true.
4. It is computationally infeasible for any entity other than A to find, for any m ∈ M, an s ∈ S such that VA (m, s) = true.m (DSA).

Breaking Ciphers

- For as long as ciphers have existed, there have been people trying to break them.
- There are many methods employed to break cipher from are ingenious, sophisticated and technical in nature, while others are more crude in nature.
- The following sections describe some of the more widely used techniques employed in breaking

ciphers.

1. **Known Plaintext Attack**

- This method relies on the code breaker knowing in advance the plaintext content of a ciphertext message.
- Having both the plaintext and the ciphertext the code breaker reengineers the cipher and the key used to create the ciphertext.

2. **Chosen Plaintext Attack**

- This method relies on the ability of the code breaker to somehow get a chosen plaintext message encrypted.
- During World War II the United States used a variation of this method to ascertain the plans of the Japanese navy in the Pacific.
- The United States had some success in breaking the Japanese codes. The U.S. Navy had determined that the Japanese were planning to attack a location referred to in their transmissions as "AF." The United States suspected that site AF was Midway Island.
- To determine if AF was, in fact, Midway, the United States ordered that a message be transmitted from Midway stating that the island's water condenser had broken down. The message was to be sent in the clear so that there would be no chance that the Japanese could not intercept it.
- Sure enough the Japanese took the bait. A few days later, the United States intercepted a Japanese coded message stating that AF's water condenser had failed.

1. Cryptanalysis

- Technically, any method employed to break a cipher or code is cryptanalysis. Today cryptanalysis employing mathematical analysis to break a code.
- This method requires a high level of skill and sophistication. It is usually only employed by academics and governments. Today it relies very heavily on the use of ultrafast super computers.
- Probably the most active and successful organization in the world, dedicated to breaking codes, is the **National Security Agency (NSA).**
- This is the largest and most secret spy agency in the United States. It is sometimes referred to as the Puzzle Palace, because the group spends so much time and energy on codes and cipher. The NSA employs tens of thousands of people.
- The only comparable organization in the world ever to have existed in terms of size is the former Soviet Union's KGB.

1. Brute Force

- The brute force method tries every possible combination of keys or algorithms to break a cipher.
- Doing so can require tremendous resources. Usually, this type of attack requires computer assistance.
    - ○ If the algorithm is simple or the key is small, then the CPU resources required could be

provided by a simple PC.

  - ○ If the algorithm is sophisticated or the key is large, then advanced computing power might be required.

1. Social Engineering

- This method relies on breaking a cipher by getting someone knowledgeable about the cipher to reveal information on how to break it.
- Bribing someone, tricking him or heExamples of widely deployed symmetric key cryptosystems include DES,
- IDEA, Blowfish, RC4, CAST, and SKIPJACK.r into divulging information, or threatening him or her with harm can reveal information.
- When the threat of harm is employed it is sometimes referred to as **rubber-hose cryptanalysis.**

Substitution:

- This is a type of replay attack where a previous message, in part or in whole, is inserted into a legitimate message.
- An attacker does not need to break the cipher for this type of attack to be effective.

Timing Attacks:

- Some cryptosystems can be broken if an outsider is able to accurately measure the time required to perform the encryption and decryption of a known ciphertext.
- The known ciphertext and the timing provide enough information to deduce fixed exponents and factors of some systems.
- This vulnerability is mostly theoretical. If an attacker has enough access to a network to be able to accurately measure the time required to encrypt and decrypt information, then there are and problems to worry about.

Symmetric-key vs. public-key cryptography

Symmetric-key and public-key encryption schemes have various advantages and disadvantages, some of which are common to both.

Advantages of symmetric-key cryptography

1. Symmetric-key ciphers can be designed to have high rates of data throughput. Some hardware implementations achieve encrypt rates of hundreds of megabytes per second, while software implementations may attain throughput rates in the megabytes per second range.
2. Keys for symmetric-key ciphers are relatively short.
3. Symmetric-key ciphers can be employed as primitives to construct various cryptographic mechanisms including pseudorandom number generators , hash functions, and computationally efficient digital signature schemes , to name just a few.
4. Symmetric-key ciphers can be composed to produce stronger ciphers. Simple transformations which are easy to analyze, but on their own weak, can be used to construct strong product ciphers.
5. Symmetric-key encryption is perceived to have an extensive history, although it must be acknowledged that, notwithstanding the invention of rotor machines earlier, much of the knowledge in this area has been acquired subsequent to the invention of the digital computer, and, in particular, the design of the Data Encryption Standard in the early 1970s.

Disadvantages of symmetric-key cryptography

1. In a two-party communication, the key must remain secret at both ends.
2. In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an unconditionally trusted TTP .
3. In a two-party communication between entities A and B, sound cryptographic practice dictates that the key be changed frequently, and perhaps for each communication session.
4. Digital signature mechanisms arising from symmetric-key encryption typically require either large keys for the public verification function or the use of a TTP .

Advantages of public-key cryptography

1. Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed).
2. The administration of keys on a network requires the presence of only a functionally trusted TTP (Definition 1.66) as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an “off-line” manner, as opposed to in real time.
3. Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years).
4. Many public-key schemes yield relatively efficient digital signature mechanisms.
5. In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

6. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart.

Disadvantages of public-key encryption

1. Throughput rates for the most popular public-key encryption methods are several orders of magnitude slower than the best known symmetric-key schemes.
2. Key sizes are typically much larger than those required for symmetric-key encryption (, and the size of public-key signatures is larger than that of tags providing data origin authentication from symmetric-key techniques.
3. No public-key scheme has been proven to be secure (the same can be said for block ciphers). The most effective public-key encryption schemes found to date have their security based on the presumed difficulty of a small set of number-theoretic problems.
4. Public-key cryptography does not have as extensive a history as symmetric-key encryption, being discovered only in the mid 1970s.

APPENDIX Security Elements Key terms

1. *Access control list (ACL) :* A list of individual users and groups of users associated with an object, and the rights that the user or group has when accessing that object.
2. *Algorithm:*A computable set of steps to achieve a desired result.
3. *Asymmetric encryption:* A type of encryption that uses one key to encrypt a message and another to decrypt the message. (Also, public-key encryption)
4. *Authentication:* The process of identifying an individual, usually based on a username and password.
5. *Back door:* An intentional hole in a firewall or security apparatus that allows access around security measures.
6. *Ciphertext:* Text which has been encrypted by some encryption system.
7. *Data confidentiality:* The degree of confidentiality required for data transmitted, correlating to the security measures required to maintain confidentiality. Data confidentiality is provided by encryption.
8. *Encryption:* The process of disguising a message to make it unreadable by humans. The resulting data is called ciphertext.
9. *Execution control list (ECL):* A list of the resources and actions which a program can access/perform while it is executing.
10. *Hash algorithm:* A numeric function which mixes the ordering of input values to hopefully get an even distribution. (Also, hash function)
11. *Key:* A method of opening an encryption. A key can be as simple as a string of text characters, or a series of hexadecimal digits.
12. *Non-repudiation:* The ability to demonstrate that an information exchange or financial transaction took place.
13. One-way encryption: A type of encryption where information is encrypted once and cannot be decrypted. One-way encryption is typically used for creating message digests.

14. *Secure HTTP (SHTTP)*
15. *Secure Multipurpose Internet Mail Extension (S/MIME)*
16. *Secure Sockets Layer (SSL)*
17. *Security mechanisms*
18. Security service: A basic method for providing data security. Security services include authentication, access control, data integrity, data confidentiality, and nonrepudiation.
19. Symmetric encryption:A type of encryption where the same key is used to encrypt and decrypt the message.
20. Virtual Private Network (VPN): An extended local area network (LAN) that enables an organization to conduct secure, real-time communication.