# SEGURIDAD INFORMÁTICA

# Unidad 2:

# CRIPTOGRAFÍA

# Objetivo de la Unidad de Aprendizaje:

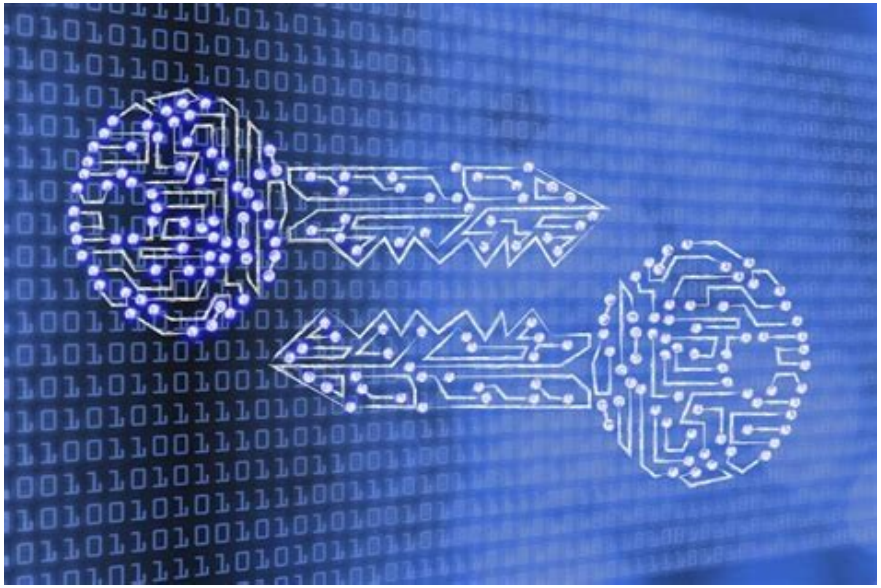
El alumno desarrollará aplicaciones de software integrando algoritmos criptográficos para mantener la confidencialidad de la información.

**Temas:**

- Algoritmos de cifrado
- Algoritmos hash

# Criptografía.

**La criptografía** surge como una necesidad para realizar comunicaciones por escrito (en su origen) y creada para preservar la privacidad de la información que se transmite, garantizando que una persona que no esté autorizada no puede leer el contenido del mensaje.



# Criptografía.

## Criptografía simétrica

La criptografía simétrica sólo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente y este es el punto débil del sistema, la comunicación de las claves entre ambos sujetos, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad


## Criptografía asimétrica

La criptografía asimétrica se basa en el uso de dos claves: la pública (que se podrá difundir sin ningún problema a todas las personas que necesiten enviarte algo cifrado) y la privada (no debe de ser revelada nunca).


## Criptografía híbrida

Este sistema es la unión de las ventajas de los dos anteriores, ya que el método simétrico es inseguro y el asimétrico es lento.

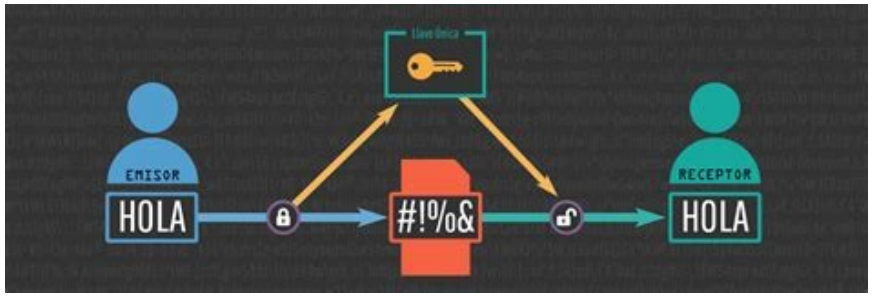
# Criptografía.

**DEFINICIONES**

**Criptología:** proviene del griego krypto, “oculto”, y logos, “estudio”. Se trata del estudio de los criptosistemas. Sus áreas principales de estudio son, entre otros, la criptografía y el criptoanálisis:

- **Criptografía:** proviene del griego krypto, “oculto”, y graphos, “escribir”; es decir, significa “escritura oculta”. El diccionario de la RAE lo define como “el arte de escribir con clave secreta o de un modo enigmático”. La criptografía no pretende ocultar un mensaje, sino únicamente su significado, a través de la codificación.

- **Criptoanálisis:** es la ciencia que se ocupa de descifrar criptogramas rompiendo la clave utilizada para descubrir el contenido del mensaje. Es el reverso de la criptografía.




**Criptosistema:** según el Centro Criptológico Nacional (CCN), es el conjunto de claves y equipos de cifra que utilizados coordinadamente, ofrecen un medio para cifrar y descifrar**.**

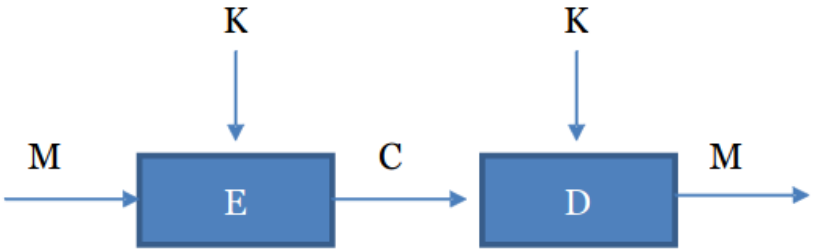
**Cifrar:** transcribir, utilizando una clave, un mensaje cuyo contenido se quiere ocultar.

**Clave:** conjunto de signos utilizados para la transmisión de un mensaje privado cuyo contenido se quiere ocultar.

# Criptografía.

**Los elementos que forman parte de un criptosistema son:**

- **M:** que representa el mensaje o texto en claro, que por sí solo es legible o interpretable (caso de un programa o aplicación) por cualquier entidad.
- **C:** que representa al criptograma, esto es el texto cifrado que se trasmitirá por el canal de comunicación, el cual por definición es inseguro y por ello es necesario cifrar la información.
- **E:** que representa la función de cifrado que se aplica al texto en claro. La letra E proviene del inglés Encrypt.
- **D:** que representa la función de descifrado que se aplica al texto cifrado para recuperar el texto en claro. La letra D proviene del inglés Decrypt.
- **K:** que representa la clave empleada para cifrar el texto en claro M,o bien para descifrar el criptograma C. En los sistemas modernos de cifrado asimétrica o de clave pública, estas claves K serán diferentes en ambos extremos.

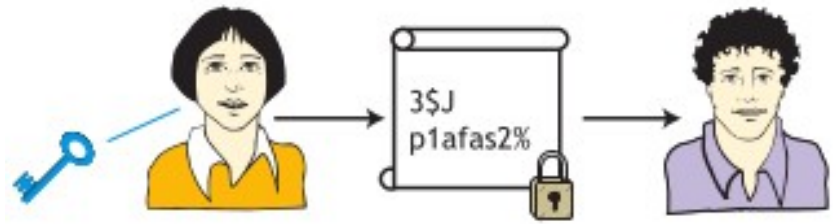


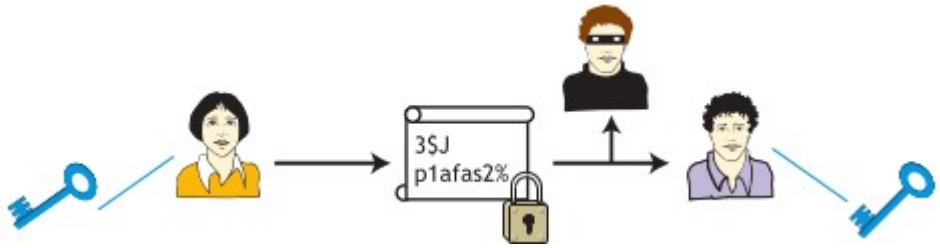

Esquema de un criptosistema clásico.

# Criptografía.

## Cifrado de clave simétrica

- Estos sistemas se utilizala misma clave para cifrar y descifrar un mensaje. Dicha clave solo deberá ser conocida por el emisor y el receptor del mensaje y deberá mantenerse en secreto.
- **Hay dos grandes grupos de algoritmos de cifrado:**
  - **Cifradores de flujo:** cifran bit a bit.
  - **Cifradores de bloque:** cifran un bloque de bits (habitualmente, cada bloque es de 64 bits) como una unidad.
- Uno de los inconvenientes de este tipo de cifrado es que la clave debe ser conocida por el emisor y el receptor, quienes deben encontrar un modo seguro de comunicarla entre ambos.



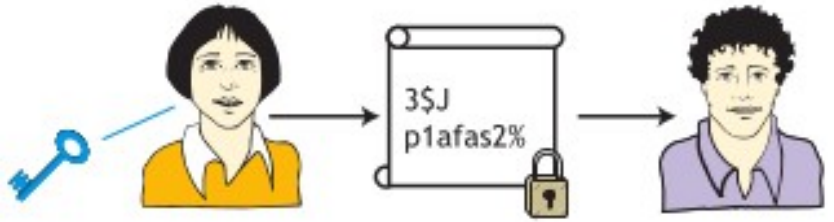



# Criptografía.

## Cifrado de clave simétrica

**Ventajas:**

- Son rápidos y eficientes.
- Resultan apropiados para el cifrado de grandes volúmenes de datos.

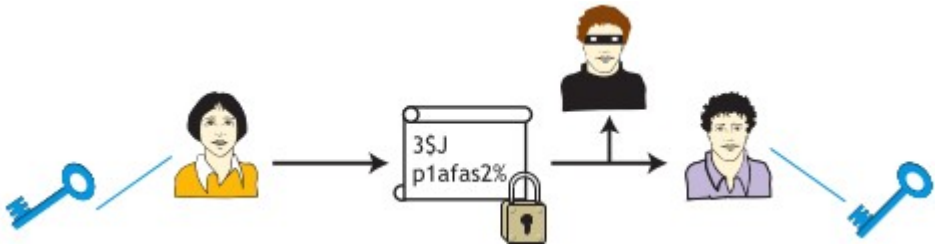



**Desventajas:**

- Exigen una clave diferente por cada pareja de interlocutores (el espacio de claves se incrementa enormemente conforme aumentan los interlocutores).

- Requiere un control estricto sobre el intercambio seguro de la clave entre el emisor y el receptor.

- Son vulnerables a ataques por fuerza bruta, por lo que la fortaleza de la clave es fundamental.



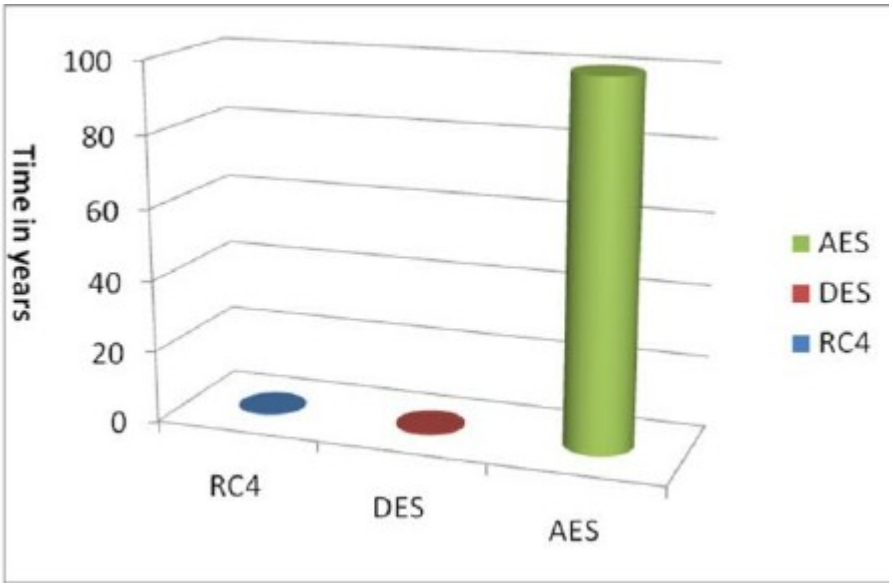
# Criptografía.

## Algoritmos de cifrado para clave simétricas

### DES (Data Encryption Standard)

- Utiliza cifrado por bloques con bloques de 64 bits, esto es, toma un texto plano de esa longitud y lo transforma, mediante una serie de operaciones, en texto cifrado de la misma longitud.

- Se utilizan claves de 64 bits, de los cuales solo se utilizan 56, para realizar el cifrado de los bloques. El resto llevan información de paridad. Esta longitud tan corta se considera insuficiente para protegerse frente a ataques de fuerza bruta y es uno de los motivos por los que se considera inseguro, ya que estas claves se han llegado a romper en 24 horas. Aun así se sigue utilizando en las transacciones realizadas en cajeros automáticos.




### Triple DES

- Triple DES aumenta la seguridad de DES ejecutando el algoritmo DES tres veces, cada una de ellas con una clave distinta.

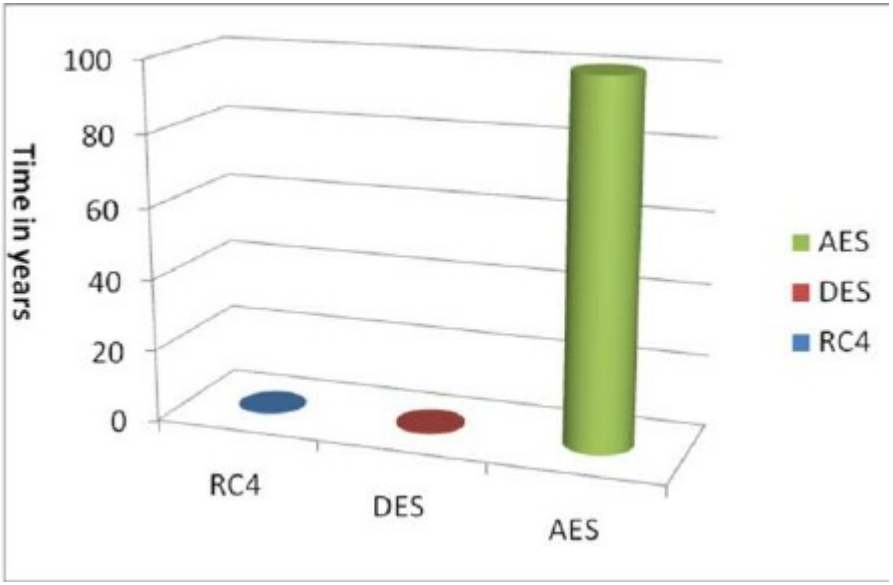
# Criptografía.

## Algoritmos de cifrado para clave simétricas

### AES (Advanced Encryption Standard)

- El estándar de encriptación avanzada es uno de los algoritmos más populares de clave simétrica y, de hecho, remplazará al DES utilizado habitualmente.

- Es rápido y eficiente y proporciona una encriptación segura utilizando un cifrado por bloques, con bloques de 128 bits y claves de 128, 192 o 256 bits. Se utiliza fundamentalmente en aplicaciones bancarias por Internet, comunicaciones inalámbricas, protección de datos en discos duros, etc



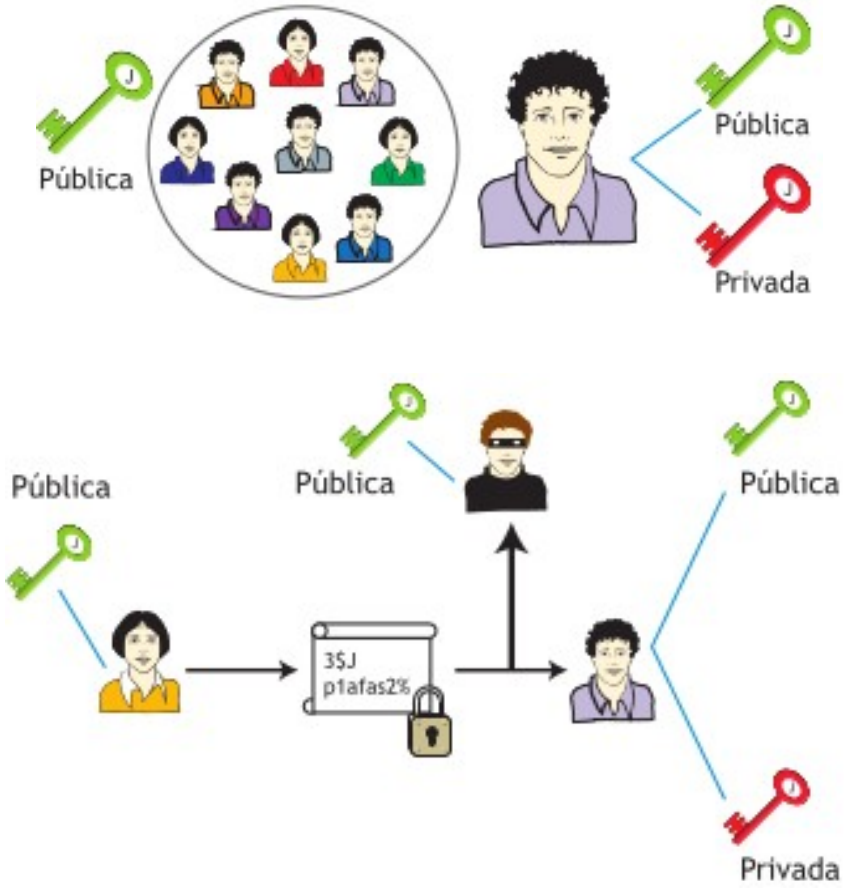
# Criptografía.

## Cifrado de clave asimétrica

- Cuando alguien quiera cifrar un mensaje dirigido, utilizará la clave pública (que es conocida) para cifrarlo, pero únicamente se podrá leer, el que posea la clave privada. Funcionaría de forma similar a un candado, cualquiera puede cerrarlo, pero solo quien tenga la llave de ese candado puede abrirlo.

- La criptografía asimétrica tiene dos usos principales:

    - Autenticación.
    - Confidencialidad.



# Criptografía.

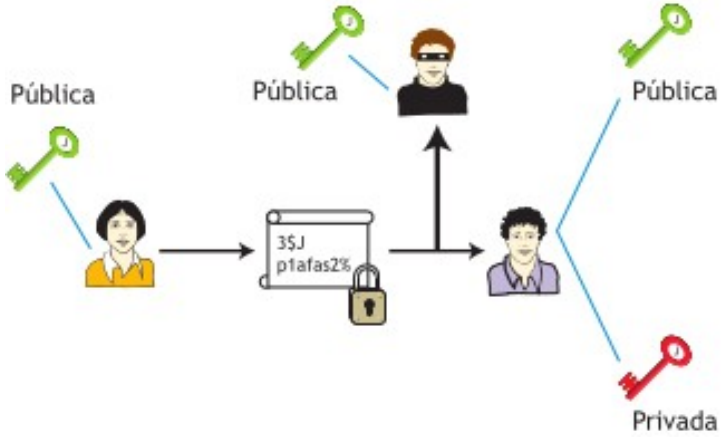
## Cifrado de clave asimétrica

### Ventajas:

- La clave pública se distribuye libremente, por lo que ya no existe el problema del intercambio de la clave que había en los métodos simétricos.
- Solo es necesario un par de claves por interlocutor, con independencia del número de estos, por lo que el espacio de claves es más manejable cuando los interlocutores son muchos.


### Desventajas:

- Requieren mayor tiempo de proceso que el cifrado simétrico.
- Dan lugar a mensajes cifrados de mayor tamaño que los originales.
- Para garantizar la seguridad, requieren claves de mayor tamaño que en el caso de los métodos simétricos.
- Puesto que las claves públicas se distribuyen libremente, hace falta un esquema de confianza que garantice la autenticidad de las claves públicas (que la clave pública sea de quien dice que es, que no ha sido comprometida, etc.).



# Criptografía.

## Los algoritmos de cifrado asimétrico

### RSA (Rivest-Shamir-Adelman)

- Fue creado en 1977 y es uno de los algoritmos más utilizados. Permite cifrar y firmar digitalmente, aunque es mucho más lento que DES y que otros sistemas de cifrado de clave simétrica


### DSA (Digital Signature Algorithm)

- Algoritmo de firma digital, estándar del Gobierno Federal de Estados Unidos. Para entornos críticos, se ha demostrado que DSA es más seguro que RSA. Permite firmar digitalmente, sin embargo no permite cifrar la información.

### ElGamal

- Fue escrito por Taher ElGamal en 1984. Algoritmo de uso libre utilizado en software GNU Privacy Guard, en versiones recientes de PGP. Puede ser utilizado para cifrar y firmar digitalmente, con un tiempo de cómputo similar a RSA.

# SSH

## Protección de Sistemas Operativos.

- **Servidor SSH: ¿Qué es?**

- SSH es el acrónimo de Secure Shell, y es un protocolo que se utiliza en el manejo de servidores de forma remota, permitiendo a un usuario realizar toda clase de tareas sobre el mismo.

- En las conexiones realizadas por medio de SSH, toda la información viaja de forma encriptada, lo cual lo convierte en uno de los medios más seguros a la hora de trabajar en un servidor.

# SSH

## Protección de Sistemas Operativos.

### Uso de SSH

- **Copiado de datos:** con el protocolo SSH podemos copiar datos, esto se puede lograr por ejemplo mediante herramientas como rsync o scp.

- **Ejecución de comandos remotos:** lograr ejecutando una sintaxis en nuestro terminal o, si el comando es complejo, mediante un script en bash.

- **Multiplexación en SSH:** si bien no es usado comúnmente, con SSH se puede realizar una multiplexación, es decir, crear varias sesiones de SSH mediante una sola conexión TCP.

# SSH

## Protección de Sistemas Operativos.

### Tipos de Encriptación SSH

- **Cifrado simétrico:** También denominado “Shared Key” o “Shared Secret” en determinados campos, se caracteriza por el uso de una única llave tanto para cifrar como para descifrar la información.



- **Cifrado asimétrico:** se le conoce como “Criptografía de Llave Pública”. La principal diferencia con respecto al cifrado simétrico radica en que en este caso son necesarias dos llaves; una para el cifrado de la información y otra para el descifrado de la misma.

# SSH

## Protección de Sistemas Operativos.

### Tipos de Encriptación SSH

- **Hashing:** conexión cifrada con un hash no puede ser revertida, es prácticamente única y casi imposible de predecir, de hecho solo el servidor que recibirá los datos será capaz de leerlos correctamente. Las conexiones cifradas mediante hash se logran convirtiendo la información en una nueva cadena de datos que poseen una cierta longitud que jamás cambia.