CÓDIGOS Y CRIPTOGRAFÍA

Una breve historia de la criptografía. Conceptos básicos

En nuestro partido político
cumplimos con lo que prometemos.
Sólo los imbéciles pueden creer que
no lucharemos contra la corrupción.
Porque si hay algo seguro para nosotros es que
la honestidad y la transparencia son fundamentales
para alcanzar nuestros ideales.
Demostraremos que es una gran estupidez creer que
las mafias seguirán formando parte del gobierno como en otros tiempos.
Aseguramos sin resquicio de duda que
la justicia social será el fin principal de nuestro mandato.
Pese a eso, todavía hay gente estúpida que piensa que
se pueda seguir gobernando con las artimañas de la vieja política.
Cuando asumamos el poder, haremos lo imposible para que
se acaben las situaciones privilegiadas y el tráfico de influencias
No permitiremos de ningún modo que
nuestros niños mueran de hambre.
Cumpliremos nuestros propósitos aunque
los recursos económicos se hayan agotado
ejerceremos el poder hasta que
Comprendan desde ahora que
Somos el Partido XXX, "la nueva política".

Berto Romero, Buenafuente

Vas a entender
Ahora y de una vez
La verdad que no cuento
El motivo es mi riesgo
Me equivoqué
Urdiendo en un papel
Seis mil versos vacíos
Inocentes y fríos
Conoces mi ansiedad y mi deseo
No te importa mis miedos
Observas de reojo la herida que
Cierra en falso el dolor

Revelo así
En lo que escribo aquí
El secreto escondido
En mis versos prendido
Ni el tiempo ni el correr de los años
Me ahorrará desengaños
Intento cada día un futuro que
Ya no puedo asumir
Qué decir ante el porvenir
Uniré otra vez lo que destrocé
Éste es el final.

Vas a entender, Naím Thomas

Ocultando mensajes

Ocultando mensajes

ESTEGANOGRAFÍA

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo

encubierto + escritura

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo
encubierto + escritura

- La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros de modo que no se perciba su existencia.

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo
encubierto + escritura

- La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros de modo que no se perciba su existencia.

* Crónicas de Herodoto, s. V a.C: Demarato salvó a Grecia de la ocupación persa con tablillas de madera enceradas.

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo
encubierto + escritura

- La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros de modo que no se perciba su existencia.

* Crónicas de Herodoto, s. V a.C: Demarato salvó a Grecia de la ocupación persa con tablillas de madera enceradas.
* El militar Histaiaeo enviaba mensajes ocultos en el cuero cabelludo de los soldados. Origen de las guerras Médicas.

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo
encubierto + escritura

- La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros de modo que no se perciba su existencia.

* Crónicas de Herodoto, s. V a.C: Demarato salvó a Grecia de la ocupación persa con tablillas de madera enceradas.
* El militar Histaiaeo enviaba mensajes ocultos en el cuero cabelludo de los soldados. Origen de las guerras Médicas.
* El historiador Eneas el Estratega comunica mensajes con agujeros diminutos bajo las letras de un texto.

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo
encubierto + escritura

- La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros de modo que no se perciba su existencia.

* Crónicas de Herodoto, s. V a.C: Demarato salvó a Grecia de la ocupación persa con tablillas de madera enceradas.
* El militar Histaiaeo enviaba mensajes ocultos en el cuero cabelludo de los soldados. Origen de las guerras Médicas.
* El historiador Eneas el Estratega comunica mensajes con agujeros diminutos bajo las letras de un texto.
* Antigua civilización china. Se escribían los mensajes sobre seda fina recubierta de seda.

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo
encubierto + escritura

- La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros de modo que no se perciba su existencia.

* Crónicas de Herodoto, s. V a.C: Demarato salvó a Grecia de la ocupación persa con tablillas de madera enceradas.
* El militar Histaiaeo enviaba mensajes ocultos en el cuero cabelludo de los soldados. Origen de las guerras Médicas.
* El historiador Eneas el Estratega comunica mensajes con agujeros diminutos bajo las letras de un texto.
* Antigua civilización china. Se escribían los mensajes sobre seda fina recubierta de seda.
* Plinio el Viejo, s. I. Mensaje con tinta invisible.

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo
encubierto + escritura

- La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros de modo que no se perciba su existencia.

* Crónicas de Herodoto, s. V a.C: Demarato salvó a Grecia de la ocupación persa con tablillas de madera enceradas.
* El militar Histaiaeo enviaba mensajes ocultos en el cuero cabelludo de los soldados. Origen de las guerras Médicas.
* El historiador Eneas el Estratega comunica mensajes con agujeros diminutos bajo las letras de un texto.
* Antigua civilización china. Se escribían los mensajes sobre seda fina recubierta de seda.
* Plinio el Viejo, s. I. Mensaje con tinta invisible.
* Giovanni de la Porta, s. XV. Mensaje oculto en un huevo cocido.

Ocultando mensajes

ESTEGANOGRAFÍA

steganos + grafo
encubierto + escritura

- La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros de modo que no se perciba su existencia.

* Crónicas de Herodoto, s. V a.C: Demarato salvó a Grecia de la ocupación persa con tablillas de madera enceradas.
* El militar Histaiaeo enviaba mensajes ocultos en el cuero cabelludo de los soldados. Origen de las guerras Médicas.
* El historiador Eneas el Estratega comunica mensajes con agujeros diminutos bajo las letras de un texto.
* Antigua civilización china. Se escribían los mensajes sobre seda fina recubierta de seda.
* Plinio el Viejo, s. I. Mensaje con tinta invisible.
* Giovanni de la Porta, s. XV. Mensaje oculto en un huevo cocido.
* En la actualidad: tinta invisible, esteganografía digital...

Ocultando significados

CRIPTOGRAFÍA

Ocultando significados

CRIPTOGRAFÍA

kryptos + grafo

escondido + escritura

Ocultando significados

CRIPTOGRAFÍA

kryptos + grafo
escondido + escritura

- Según la RAE, la criptografía es el arte de escribir con clave secreta o de un modo enigmático.

Ocultando significados

CRIPTOGRAFÍA

kryptos + grafo
escondido + escritura

- Según la RAE, la criptografía es el arte de escribir con clave secreta o de un modo enigmático.

La definición anterior no es buena actualmente porque:

Ocultando significados

CRIPTOGRAFÍA

kryptos + grafo
escondido + escritura

- Según la RAE, la criptografía es el arte de escribir con clave secreta o de un modo enigmático.

La definición anterior no es buena actualmente porque:

- *es el arte*. No sólo es un arte, también una ciencia.

Ocultando significados

CRIPTOGRAFÍA

kryptos + grafo
escondido + escritura

- Según la RAE, la criptografía es el arte de escribir con clave secreta o de un modo enigmático.

La definición anterior no es buena actualmente porque:

- *es el arte*. No sólo es un arte, también una ciencia.
- *de escribir*. No sólo se escribe, se usa en documentos de imagen, de sonido...

Ocultando significados

CRIPTOGRAFÍA

kryptos + grafo
escondido + escritura

- Según la RAE, la criptografía es el arte de escribir con clave secreta o de un modo enigmático.

La definición anterior no es buena actualmente porque:

- *es el arte*. No sólo es un arte, también una ciencia.
- *de escribir*. No sólo se escribe, se usa en documentos de imagen, de sonido...
- *con clave secreta*. Los sistemas más usados hoy en día son de clave pública.

Ocultando significados

CRIPTOGRAFÍA

kryptos + grafo
escondido + escritura

- Según la RAE, la criptografía es el arte de escribir con clave secreta o de un modo enigmático.

La definición anterior no es buena actualmente porque:

- *es el arte*. No sólo es un arte, también una ciencia.
- *de escribir*. No sólo se escribe, se usa en documentos de imagen, de sonido...
- *con clave secreta*. Los sistemas más usados hoy en día son de clave pública.
- *de un modo enigmático*. Actualmente el alfabeto de crifrado consiste en bits, es decir, ceros y unos, lo cual no es ningún enigma.

Ocultando significados

CRIPTOGRAFÍA

kryptos + grafo
escondido + escritura

- Según la RAE, la criptografía es el arte de escribir con clave secreta o de un modo enigmático.

Una definición alternativa

La criptografía es una rama de las Matemáticas, y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Ocultando y desvelando

CRIPTOANÁLISIS

Ocultando y desvelando

CRIPTOANÁLISIS

kryptos + analyein

escondido + desatar

Ocultando y desvelando

CRIPTOANÁLISIS

kryptos + analyein
escondido + desatar

- El criptoanálisis se dedica al estudio de técnicas destinadas al análisis de la información cifrada para recuperar el mensaje original.

Ocultando y desvelando

CRIPTOANÁLISIS

kryptos + analyein
escondido + desatar

- El criptoanálisis se dedica al estudio de técnicas destinadas al análisis de la información cifrada para recuperar el mensaje original.

- Los orígenes del criptoanálisis se hallan en los árabes. En el siglo X tenían manuales como el "Adab al-Kuttb".

Ocultando y desvelando

CRIPTOANÁLISIS

kryptos + analyein
escondido + desatar

- El criptoanálisis se dedica al estudio de técnicas destinadas al análisis de la información cifrada para recuperar el mensaje original.

- Los orígenes del criptoanálisis se hallan en los árabes. En el siglo X tenían manuales como el "Adab al-Kuttb".

CRIPTOLOGÍA

Ocultando y desvelando

CRIPTOANÁLISIS

kryptos + analyein
escondido + desatar

- El criptoanálisis se dedica al estudio de técnicas destinadas al análisis de la información cifrada para recuperar el mensaje original.

- Los orígenes del criptoanálisis se hallan en los árabes. En el siglo X tenían manuales como el "Adab al-Kuttb".

CRIPTOLOGÍA: CRIPTOGRAFÍA + CRIPTOANÁLISIS

Ocultando y desvelando

CRIPTOANÁLISIS

kryptos + analyein
escondido + desatar

- El criptoanálisis se dedica al estudio de técnicas destinadas al análisis de la información cifrada para recuperar el mensaje original.

- Los orígenes del criptoanálisis se hallan en los árabes. En el siglo X tenían manuales como el "Adab al-Kuttb".

CRIPTOLOGÍA: CRIPTOGRAFÍA + CRIPTOANÁLISIS

- La historia de la criptología se puede entender como una lucha entre criptógrafos y criptoanalistas.

Ocultando y desvelando

CRIPTOANÁLISIS

kryptos + analyein
escondido + desatar

- El criptoanálisis se dedica al estudio de técnicas destinadas al análisis de la información cifrada para recuperar el mensaje original.

- Los orígenes del criptoanálisis se hallan en los árabes. En el siglo X tenían manuales como el "Adab al-Kuttb".

CRIPTOLOGÍA: CRIPTOGRAFÍA + CRIPTOANÁLISIS

- La historia de la criptología se puede entender como una lucha entre criptógrafos y criptoanalistas.
- Históricamente siempre han ganado los criptoanalistas.

Ocultando y desvelando

CRIPTOANÁLISIS

kryptos + analyein
escondido + desatar

- El criptoanálisis se dedica al estudio de técnicas destinadas al análisis de la información cifrada para recuperar el mensaje original.

- Los orígenes del criptoanálisis se hallan en los árabes. En el siglo X tenían manuales como el "Adab al-Kuttb".

CRIPTOLOGÍA: CRIPTOGRAFÍA + CRIPTOANÁLISIS

- La historia de la criptología se puede entender como una lucha entre criptógrafos y criptoanalistas.
- Históricamente siempre han ganado los criptoanalistas.
- Esta tendencia se está cambiando en la actualidad gracias a la influencia de las matemáticas.

Un poco de historia

- Hace 4000 años, se encuentran los primeros mensajes codificados en los jeroglíficos egipcios. El primero conocido data del año 1900 a.C.

Un poco de historia

- Hace 4000 años, se encuentran los primeros mensajes codificados en los jeroglíficos egipcios. El primero conocido data del año 1900 a.C.
- El primer aparato criptográfico de la historia es el escítalo o escítala, en el s. V a.C. en la antigua Grecia.

Un poco de historia

- Hace 4000 años, se encuentran los primeros mensajes codificados en los jeroglíficos egipcios. El primero conocido data del año 1900 a.C.
- El primer aparato criptográfico de la historia es el escítalo o escítala, en el s. V a.C. en la antigua Grecia.
- El cifrador por sustitución de caracteres más antiguo se debe al historiador griego Polybios en el s. II a.C.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N	Ñ	O
D	P	Q	R	S	T
E	U	V	WX	Y	Z

Un poco de historia

- Hace 4000 años, se encuentran los primeros mensajes codificados en los jeroglíficos egipcios. El primero conocido data del año 1900 a.C.
- El primer aparato criptográfico de la historia es el escítalo o escítala, en el s. V a.C. en la antigua Grecia.
- El cifrador por sustitución de caracteres más antiguo se debe al historiador griego Polybios en el s. II a.C.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N	Ñ	O
D	P	Q	R	S	T
E	U	V	WX	Y	Z

- En el texto Kama-Sutra (Vatsyayana, s. IV d.C. basado en textos del s. IV a.C.) se recomienda a las mujeres el arte de la escritura secreta.

Un poco de historia

- Hace 4000 años, se encuentran los primeros mensajes codificados en los jeroglíficos egipcios. El primero conocido data del año 1900 a.C.
- El primer aparato criptográfico de la historia es el escítalo o escítala, en el s. V a.C. en la antigua Grecia.
- El cifrador por sustitución de caracteres más antiguo se debe al historiador griego Polybios en el s. II a.C.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N	Ñ	O
D	P	Q	R	S	T
E	U	V	WX	Y	Z

- En el texto Kama-Sutra (Vatsyayana, s. IV d.C. basado en textos del s. IV a.C.) se recomienda a las mujeres el arte de la escritura secreta.
- El cifrado del César fue usado con própositos militares por Julio César, s. I a.C.

Un poco de historia

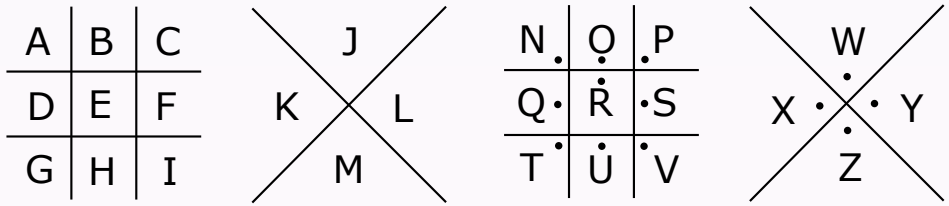
- El libro más antiguo sobre criptografía conocido es el Liber Zifrorum escrito por Cicco Simoneta en el s. XIV.

Un poco de historia

- El libro más antiguo sobre criptografía conocido es el Liber Zifrorum escrito por Cicco Simoneta en el s. XIV.
- En el s. XV León Battista Alberti crea el disco de cifras de Alberti, usado hasta la guerra civil norteamericana.

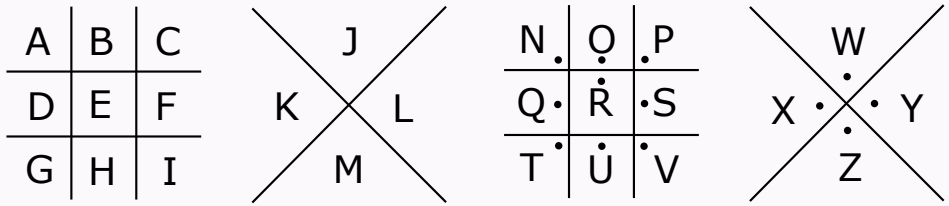
Un poco de historia

- El libro más antiguo sobre criptografía conocido es el Liber Zifrorum escrito por Cicco Simoneta en el s. XIV.
- En el s. XV León Battista Alberti crea el disco de cifras de Alberti, usado hasta la guerra civil norteamericana.
- En 1533 Heinrich Cornelius Agrippa von Nettelsheim publica De occulta philosophia. Describe la cifra Pig Pen



Un poco de historia

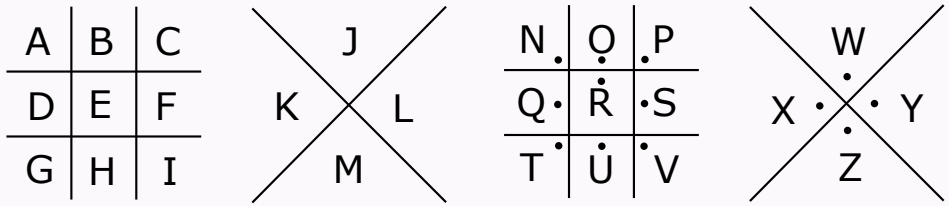
- El libro más antiguo sobre criptografía conocido es el Liber Zifrorum escrito por Cicco Simoneta en el s. XIV.
- En el s. XV León Battista Alberti crea el disco de cifras de Alberti, usado hasta la guerra civil norteamericana.
- En 1533 Heinrich Cornelius Agrippa von Nettelsheim publica De occulta philosophia. Describe la cifra Pig Pen



- En el s. XVI., Girolamo Cardano utilizó un método de tarjetas con agujeros perforados, (precursor del Braile).

Un poco de historia

- El libro más antiguo sobre criptografía conocido es el Liber Zifrorum escrito por Cicco Simoneta en el s. XIV.
- En el s. XV León Battista Alberti crea el disco de cifras de Alberti, usado hasta la guerra civil norteamericana.
- En 1533 Heinrich Cornelius Agrippa von Nettelsheim publica De occulta philosophia. Describe la cifra Pig Pen



- En el s. XVI., Girolamo Cardano utilizó un método de tarjetas con agujeros perforados, (precursor del Braile).
- Julio Verne (1825-1905) usa un cifrado por rejillas en "Matias Sandorff".

Un poco de historia

- La Cifra General de 1556 o Cifra de Felipe II, marcó la tendencia en la criptografía española durante el reinado de los Austrias.

Un poco de historia

- La Cifra General de 1556 o Cifra de Felipe II, marcó la tendencia en la criptografía española durante el reinado de los Austrias.
- La descifró el matemático francés François Viéte.

Un poco de historia

- La Cifra General de 1556 o Cifra de Felipe II, marcó la tendencia en la criptografía española durante el reinado de los Austrias.
- La descifró el matemático francés François Viéte.
- Consistía en:
  - Un **vocabulario o alfabeto**: cada letra es sustituida por un signo a escoger entre varios, las consonantes tenían dos opciones y las vocales tres.

Un poco de historia

- La Cifra General de 1556 o Cifra de Felipe II, marcó la tendencia en la criptografía española durante el reinado de los Austrias.
- La descifró el matemático francés François Viéte.
- Consistía en:
  - Un **vocabulario o alfabeto**: cada letra es sustituida por un signo a escoger entre varios, las consonantes tenían dos opciones y las vocales tres.
  - Un **silabario** de 130 sílabas: las principales sílabas de dos o tres letras son sustituidas por símbolos.

Un poco de historia

- La Cifra General de 1556 o Cifra de Felipe II, marcó la tendencia en la criptografía española durante el reinado de los Austrias.
- La descifró el matemático francés François Viéte.
- Consistía en:
  - Un **vocabulario o alfabeto**: cada letra es sustituida por un signo a escoger entre varios, las consonantes tenían dos opciones y las vocales tres.
  - Un **silabario** de 130 sílabas: las principales sílabas de dos o tres letras son sustituidas por símbolos.
  - Un **libro de códigos**: 385 términos comunes que eran sustituidos por códigos.

Un poco de historia

- Vigenère (1523-1596) publica Traicté des Chiffres donde recopila diferentes métodos de cifrado. Cabe destacar la cifra de Vigenère.

Un poco de historia

- Vigenère (1523-1596) publica Traicté des Chiffres donde recopila diferentes métodos de cifrado. Cabe destacar la cifra de Vigenère.
- Carlos I de Inglaterra y Napoleón utilizaban códigos de sustitución silábica o por bloques.

Un poco de historia

- Vigenère (1523-1596) publica Traicté des Chiffres donde recopila diferentes métodos de cifrado. Cabe destacar la cifra de Vigenère.
- Carlos I de Inglaterra y Napoleón utilizaban códigos de sustitución silábica o por bloques.
- Terzi (1631-1687) publica Prodromo all'Arte Maestra. Incluye una cifra usando notación musical, métodos de escritura para invidentes, y de enseñanza del habla a personas sordas.

Un poco de historia

- Vigenère (1523-1596) publica Traicté des Chiffres donde recopila diferentes métodos de cifrado. Cabe destacar la cifra de Vigenère.
- Carlos I de Inglaterra y Napoleón utilizaban códigos de sustitución silábica o por bloques.
- Terzi (1631-1687) publica Prodromo all'Arte Maestra. Incluye una cifra usando notación musical, métodos de escritura para invidentes, y de enseñanza del habla a personas sordas.
- Leibniz (1646-1716) inventó la máquina de calcular que trabajaba en una escala binaria. Esta escala es la precursora del código ASCII.

Un poco de historia

- Vigenère (1523-1596) publica Traicté des Chiffres donde recopila diferentes métodos de cifrado. Cabe destacar la cifra de Vigenère.
- Carlos I de Inglaterra y Napoleón utilizaban códigos de sustitución silábica o por bloques.
- Terzi (1631-1687) publica Prodromo all'Arte Maestra. Incluye una cifra usando notación musical, métodos de escritura para invidentes, y de enseñanza del habla a personas sordas.
- Leibniz (1646-1716) inventó la máquina de calcular que trabajaba en una escala binaria. Esta escala es la precursora del código ASCII.
- Thomas Jefferson (1743-1829) inventa el cilindro de Jefferson.

Un poco de historia

- Telegrama Zimmermann. El 17 de enero de 1917 Montgomery intercepta un telegrama lleno de códigos enviado por el Ministro de Relaciones Exteriores alemán buscando una alianza entre Alemania y México. Cambia las intenciones de EEUU en la Primera Guerra Mundial.

Un poco de historia

- Telegrama Zimmermann. El 17 de enero de 1917 Montgomery intercepta un telegrama lleno de códigos enviado por el Ministro de Relaciones Exteriores alemán buscando una alianza entre Alemania y México. Cambia las intenciones de EEUU en la Primera Guerra Mundial.
- La cifra ADFGVX se usó por los alemanes en la Primera Guerra Mundial.

Un poco de historia

- Telegrama Zimmermann. El 17 de enero de 1917 Montgomery intercepta un telegrama lleno de códigos enviado por el Ministro de Relaciones Exteriores alemán buscando una alianza entre Alemania y México. Cambia las intenciones de EEUU en la Primera Guerra Mundial.
- La cifra ADFGVX se usó por los alemanes en la Primera Guerra Mundial.
- La máquina Enigma inventada por Arthur Scherbius en 1923 y utilizada por los alemanes en la Segunda Guerra Mundial.

Un poco de historia

- Telegrama Zimmermann. El 17 de enero de 1917 Montgomery intercepta un telegrama lleno de códigos enviado por el Ministro de Relaciones Exteriores alemán buscando una alianza entre Alemania y México. Cambia las intenciones de EEUU en la Primera Guerra Mundial.
- La cifra ADFGVX se usó por los alemanes en la Primera Guerra Mundial.
- La máquina Enigma inventada por Arthur Scherbius en 1923 y utilizada por los alemanes en la Segunda Guerra Mundial.
- Diversas máquinas de cifrado y descifrado: Colossus, Hagelin, Hagelin C-48, Lucifer de IBM, Magic...

Un poco de historia

- Telegrama Zimmermann. El 17 de enero de 1917 Montgomery intercepta un telegrama lleno de códigos enviado por el Ministro de Relaciones Exteriores alemán buscando una alianza entre Alemania y México. Cambia las intenciones de EEUU en la Primera Guerra Mundial.
- La cifra ADFGVX se usó por los alemanes en la Primera Guerra Mundial.
- La máquina Enigma inventada por Arthur Scherbius en 1923 y utilizada por los alemanes en la Segunda Guerra Mundial.
- Diversas máquinas de cifrado y descifrado: Colossus, Hagelin, Hagelin C-48, Lucifer de IBM, Magic...
- El código navajo, utilizado por los americanos en la Segunda Guerra Mundial. Ha sido uno de los pocos que no se ha conseguido descifrar.

Un poco de historia

- Telegrama Zimmermann. El 17 de enero de 1917 Montgomery intercepta un telegrama lleno de códigos enviado por el Ministro de Relaciones Exteriores alemán buscando una alianza entre Alemania y México. Cambia las intenciones de EEUU en la Primera Guerra Mundial.
- La cifra ADFGVX se usó por los alemanes en la Primera Guerra Mundial.
- La máquina Enigma inventada por Arthur Scherbius en 1923 y utilizada por los alemanes en la Segunda Guerra Mundial.
- Diversas máquinas de cifrado y descifrado: Colossus, Hagelin, Hagelin C-48, Lucifer de IBM, Magic...
- El código navajo, utilizado por los americanos en la Segunda Guerra Mundial. Ha sido uno de los pocos que no se ha conseguido descifrar.
- El micropunto usado en la Segunda Guerra Mundial. Ejemplo de combinación de criptografía con esteganografía.

Los indios navajos

- Una tribu no infectada de alemanes.

Los indios navajos

- Una tribu no infectada de alemanes.
- Crearon palabras para los nombres de aviones (pájaros) y barcos (peces).

Los indios navajos

- Una tribu no infectada de alemanes.
- Crearon palabras para los nombres de aviones (pájaros) y barcos (peces).
- Crearon un alfabeto fonético para deletrear palabras difíciles.

Los indios navajos

- Una tribu no infectada de alemanes.
- Crearon palabras para los nombres de aviones (pájaros) y barcos (peces).
- Crearon un alfabeto fonético para deletrear palabras difíciles.

  Mensaje: Inglés $\rightarrow$ Navajo $\rightarrow$ (transmisión) $\rightarrow$ Navajo $\rightarrow$ Inglés

Los indios navajos

- Una tribu no infectada de alemanes.
- Crearon palabras para los nombres de aviones (pájaros) y barcos (peces).
- Crearon un alfabeto fonético para deletrear palabras difíciles.

  Mensaje: Inglés $\rightarrow$ Navajo $\rightarrow$ (transmisión) $\rightarrow$ Navajo $\rightarrow$ Inglés

  Ejemplo:

pacific

$\Downarrow$

pig ant cat ice fox ice cow

$\Downarrow$

bi-sodih wollachi mousi tkin mae tkin bagoshi

Los indios navajos

- Una tribu no infectada de alemanes.
- Crearon palabras para los nombres de aviones (pájaros) y barcos (peces).
- Crearon un alfabeto fonético para deletrear palabras difíciles.

  Mensaje: Inglés $\rightarrow$ Navajo $\rightarrow$ (transmisión) $\rightarrow$ Navajo $\rightarrow$ Inglés

  Ejemplo:

pacific

$\Downarrow$

pig ant cat ice fox ice cow

$\Downarrow$

bi-sodih wollachi mousi tkin mae tkin bagoshi

- La solidez se probó entregando una grabación a Inteligencia Naval:

"Tenemos una extraña sucesión de sonidos guturales, nasales, trabalenguas... no podemos transcribirlos y mucho menos descifrarlos"

Los indios navajos

- En total hubo 420 mensajeros navajos.

Los indios navajos

- En total hubo 420 mensajeros navajos.
- Al terminar la guerra se consideró información clasificada, los navajos fueron ignorados durante décadas.

Los indios navajos

- En total hubo 420 mensajeros navajos.
- Al terminar la guerra se consideró información clasificada, los navajos fueron ignorados durante décadas.
- Su código es uno de los pocos de la historia que no se ha conseguido descifrar.

Los indios navajos

- En total hubo 420 mensajeros navajos.
- Al terminar la guerra se consideró información clasificada, los navajos fueron ignorados durante décadas.
- Su código es uno de los pocos de la historia que no se ha conseguido descifrar.
- El euskera se utilizó con fines similares, y era más fluido.

Propiedades fundamentales

Propiedades comunes de todos los métodos de cifrado

- Ser invertibles para poder recuperar el texto original.

Propiedades fundamentales

Propiedades comunes de todos los métodos de cifrado

- Ser invertibles para poder recuperar el texto original.
- Los procesos de cifrado y descifrado serán rápidos y fáciles para quienes va destinado.

Propiedades fundamentales

Propiedades comunes de todos los métodos de cifrado

- Ser invertibles para poder recuperar el texto original.
- Los procesos de cifrado y descifrado serán rápidos y fáciles para quienes va destinado.
- Debe ser prácticamente imposible descifrar un criptograma para quien no posea las claves.

Propiedades fundamentales

Propiedades comunes de todos los métodos de cifrado

- Ser invertibles para poder recuperar el texto original.
- Los procesos de cifrado y descifrado serán rápidos y fáciles para quienes va destinado.
- Debe ser prácticamente imposible descifrar un criptograma para quien no posea las claves.
- Se podrán transmitir los mensajes como archivos mediante una línea de datos, almacenarlos o transferirlos. En definitiva, se necesita un soporte fiable para el mensaje.

Propiedades fundamentales

Propiedades comunes de todos los métodos de cifrado

- Ser invertibles para poder recuperar el texto original.
- Los procesos de cifrado y descifrado serán rápidos y fáciles para quienes va destinado.
- Debe ser prácticamente imposible descifrar un criptograma para quien no posea las claves.
- Se podrán transmitir los mensajes como archivos mediante una línea de datos, almacenarlos o transferirlos. En definitiva, se necesita un soporte fiable para el mensaje.
- La fortaleza del sistema reside en la imposibilidad computacional de romper la cifra o encontrar la clave secreta.

Un poco de nomenclatura

Criptosistema

Agentes

Un poco de nomenclatura

Criptosistema

Texto llano o claro y alfabeto del mensaje

Mensaje sin cifrar

Agentes

Un poco de nomenclatura

Criptosistema

Texto llano o claro y alfabeto del mensaje

Mensaje sin cifrar

Cifra

Cifra o algoritmo de cifrado
Proceso de transformación

Clave(s)

Elemento sobre el que recae la seguridad

Agentes

Un poco de nomenclatura

Criptosistema

Texto llano o claro y alfabeto del mensaje

Mensaje sin cifrar

Cifra

Cifra o algoritmo de cifrado
Proceso de transformación

Clave(s)

Elemento sobre el que recae la seguridad

Texto cifrado o criptograma y alfabeto de cifrado

Mensaje tras el cifrado

Agentes

Un poco de nomenclatura

Criptosistema

Texto llano o claro y alfabeto del mensaje

Mensaje sin cifrar

Cifra

Cifra o algoritmo de cifrado
Proceso de transformación

Clave(s)

Elemento sobre el que recae la seguridad

Texto cifrado o criptograma y alfabeto de cifrado

Mensaje tras el cifrado

Agentes

Interlocutores

Transmisor o emisor
Receptor o destinatario

Un poco de nomenclatura

Criptosistema

Texto llano o claro y alfabeto del mensaje

Mensaje sin cifrar

Cifra

Cifra o algoritmo de cifrado
Proceso de transformación

Clave(s)

Elemento sobre el que recae la seguridad

Texto cifrado o criptograma y alfabeto de cifrado

Mensaje tras el cifrado

Agentes

Interlocutores

Transmisor o emisor
Receptor o destinatario

Espía

Espía, criptoanalista o adversario

Clasificación de los criptosistemas

Por las circunstancias históricas y culturales

Por el número y tipo de claves utilizadas

Clasificación de los criptosistemas

Por las circunstancias históricas y culturales

- Criptosistemas clásicos.
- Criptosistemas modernos.

Por el número y tipo de claves utilizadas

Clasificación de los criptosistemas

Por las circunstancias históricas y culturales

- Criptosistemas clásicos.
- Criptosistemas modernos.

Por el número y tipo de claves utilizadas

- Criptosistemas simétricos o de clave secreta.
- Criptosistemas asimétricos o de clave pública.

De la criptografía clásica a la moderna

- Se suele llamar criptografía clásica a la desarrollada desde tiempos inmemoriales hasta la mitad del s. XX.

De la criptografía clásica a la moderna

- Se suele llamar criptografía clásica a la desarrollada desde tiempos inmemoriales hasta la mitad del s. XX.
- Se ha desarrollado principalmente por causas militares, especialmente durante la Primera y Segunda Guerra Mundial.

De la criptografía clásica a la moderna

- Se suele llamar criptografía clásica a la desarrollada desde tiempos inmemoriales hasta la mitad del s. XX.
  - Se ha desarrollado principalmente por causas militares, especialmente durante la Primera y Segunda Guerra Mundial.
  - Se basa principalmente en sistemas criptográficos de sustitución y transposición.

De la criptografía clásica a la moderna

- Se suele llamar criptografía clásica a la desarrollada desde tiempos inmemoriales hasta la mitad del s. XX.
  - Se ha desarrollado principalmente por causas militares, especialmente durante la Primera y Segunda Guerra Mundial.
  - Se basa principalmente en sistemas criptográficos de sustitución y transposición.
- La criptografía moderna empieza a surgir cuando las nuevas tecnologías electrónicas y digitales se adaptaron a las máquinas criptográficas.

De la criptografía clásica a la moderna

- Se suele llamar criptografía clásica a la desarrollada desde tiempos inmemoriales hasta la mitad del s. XX.
  - Se ha desarrollado principalmente por causas militares, especialmente durante la Primera y Segunda Guerra Mundial.
  - Se basa principalmente en sistemas criptográficos de sustitución y transposición.
- La criptografía moderna empieza a surgir cuando las nuevas tecnologías electrónicas y digitales se adaptaron a las máquinas criptográficas.
- El paso de una a otra lo marcan los siguientes hechos:

De la criptografía clásica a la moderna

- Se suele llamar criptografía clásica a la desarrollada desde tiempos inmemoriales hasta la mitad del s. XX.
  - Se ha desarrollado principalmente por causas militares, especialmente durante la Primera y Segunda Guerra Mundial.
  - Se basa principalmente en sistemas criptográficos de sustitución y transposición.
- La criptografía moderna empieza a surgir cuando las nuevas tecnologías electrónicas y digitales se adaptaron a las máquinas criptográficas.
- El paso de una a otra lo marcan los siguientes hechos:

1.- En el año 1948 se publica el estudio de Shannon sobre Teoría de la Información y Criptología.

De la criptografía clásica a la moderna

- Se suele llamar criptografía clásica a la desarrollada desde tiempos inmemoriales hasta la mitad del s. XX.
  - Se ha desarrollado principalmente por causas militares, especialmente durante la Primera y Segunda Guerra Mundial.
  - Se basa principalmente en sistemas criptográficos de sustitución y transposición.
- La criptografía moderna empieza a surgir cuando las nuevas tecnologías electrónicas y digitales se adaptaron a las máquinas criptográficas.
- El paso de una a otra lo marcan los siguientes hechos:

1.- En el año 1948 se publica el estudio de Shannon sobre Teoría de la Información y Criptología.

2.- En 1974 aparece el cifrado estándar DES.

De la criptografía clásica a la moderna

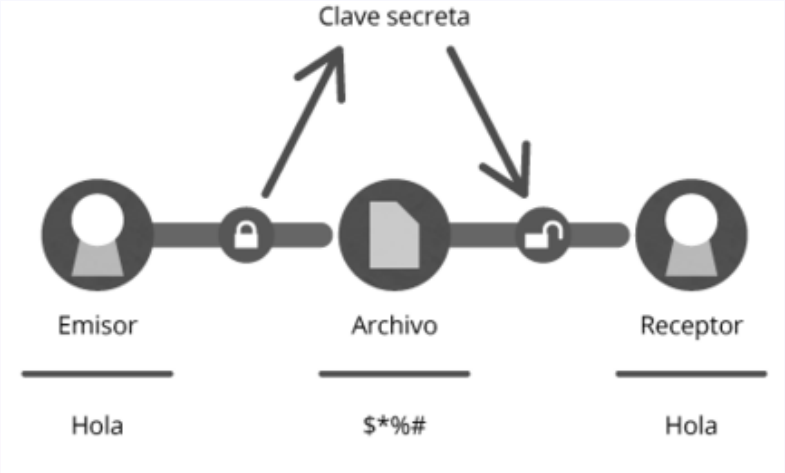
- Se suele llamar criptografía clásica a la desarrollada desde tiempos inmemoriales hasta la mitad del s. XX.
  - Se ha desarrollado principalmente por causas militares, especialmente durante la Primera y Segunda Guerra Mundial.
  - Se basa principalmente en sistemas criptográficos de sustitución y transposición.
- La criptografía moderna empieza a surgir cuando las nuevas tecnologías electrónicas y digitales se adaptaron a las máquinas criptográficas.
- El paso de una a otra lo marcan los siguientes hechos:

1.- En el año 1948 se publica el estudio de Shannon sobre Teoría de la Información y Criptología.

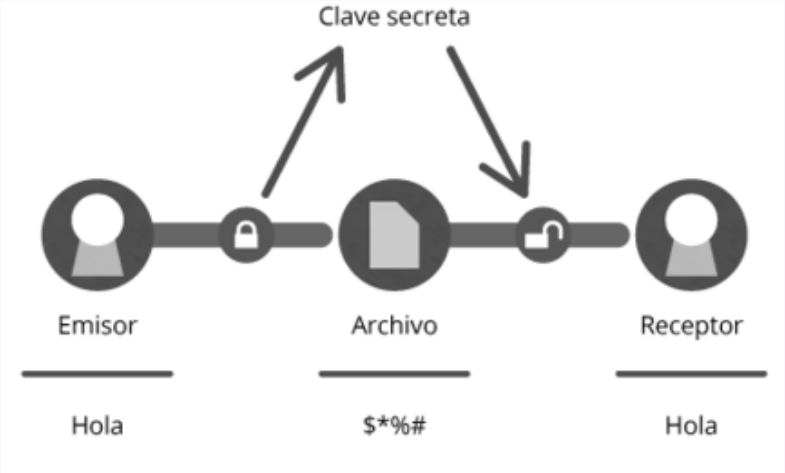
2.- En 1974 aparece el cifrado estándar DES.

3.- En 1976 Diffie y Hellman estudian la aplicación de funciones matemáticas de un sólo sentido al cifrado.

Criptosistemas simétricos o de clave secreta

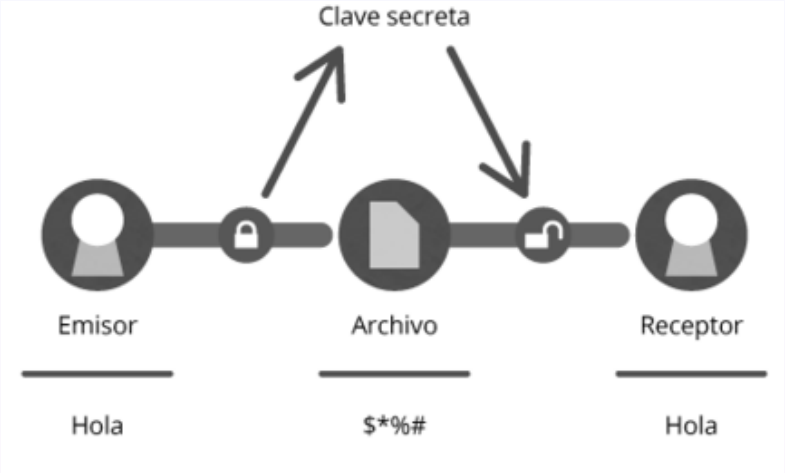


Criptosistemas simétricos o de clave secreta



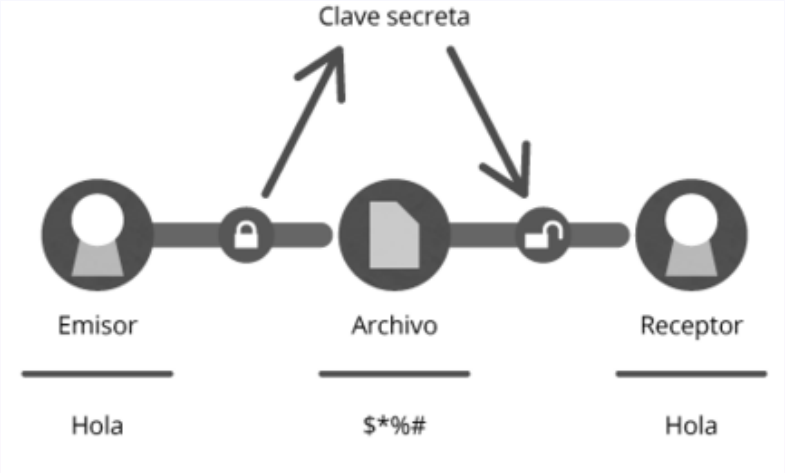
- Son propios de la Criptografía clásica.

Criptosistemas simétricos o de clave secreta



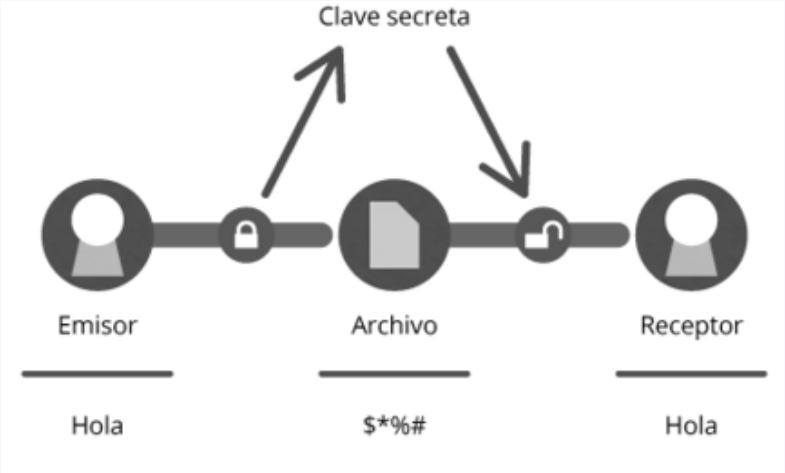
- Son propios de la Criptografía clásica.
- Existe una única clave ¡secreta! que comparten emisor y receptor.

Criptosistemas simétricos o de clave secreta



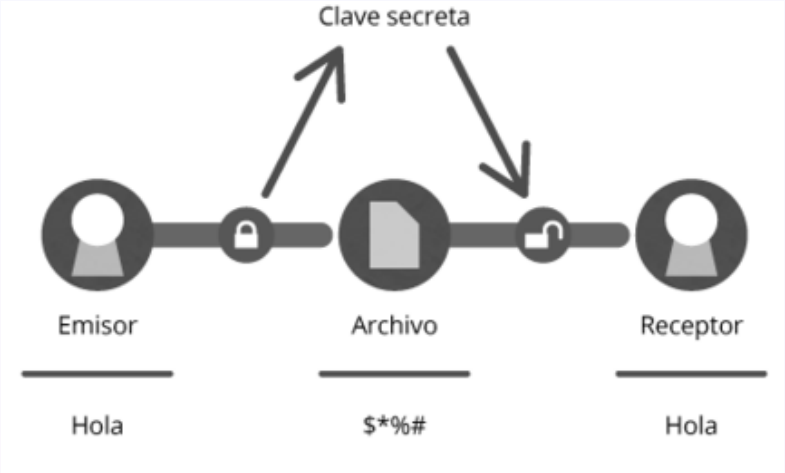
- Son propios de la Criptografía clásica.
- Existe una única clave ¡secreta! que comparten emisor y receptor.
- Es fundamental para la seguridad del método mantener dicha clave en secreto.

Criptosistemas simétricos o de clave secreta



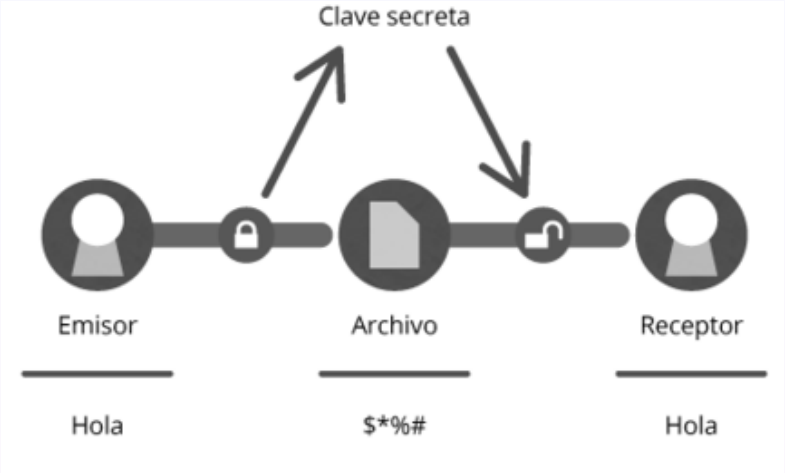
- Son propios de la Criptografía clásica.
- Existe una única clave ¡secreta! que comparten emisor y receptor.
- Es fundamental para la seguridad del método mantener dicha clave en secreto.
- Sus características principales son:
  1.- Si intervienen muchos usuarios se necesitan muchas claves. Cada par de usuarios necesita su clave secreta compartida.

Criptosistemas simétricos o de clave secreta



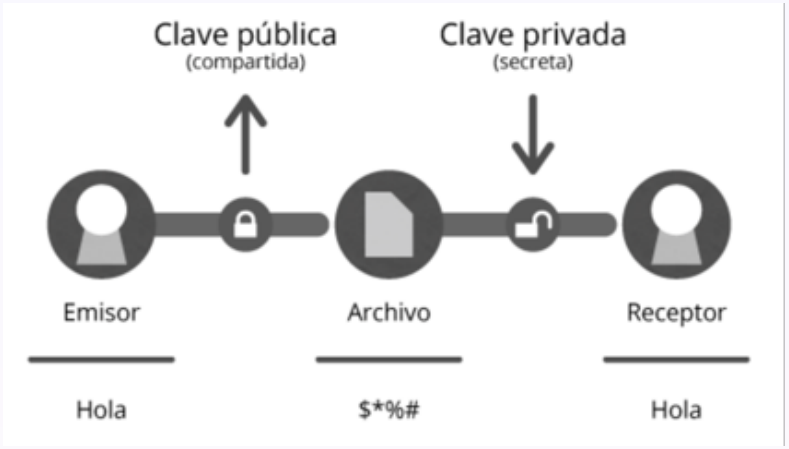
- Son propios de la Criptografía clásica.
- Existe una única clave ¡secreta! que comparten emisor y receptor.
- Es fundamental para la seguridad del método mantener dicha clave en secreto.
- Sus características principales son:
  1.- Si intervienen muchos usuarios se necesitan muchas claves. Cada par de usuarios necesita su clave secreta compartida.
  2.- Conociendo la clave de cifrado se puede descifrar fácilmente. La robustez del algoritmo recae en el secreto de la clave.

Criptosistemas simétricos o de clave secreta

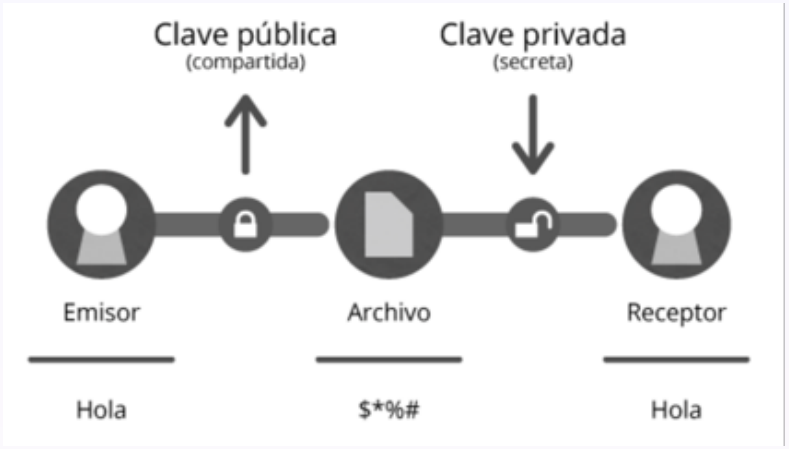


- Son propios de la Criptografía clásica.
- Existe una única clave ¡secreta! que comparten emisor y receptor.
- Es fundamental para la seguridad del método mantener dicha clave en secreto.
- Sus características principales son:
  1.- Si intervienen muchos usuarios se necesitan muchas claves. Cada par de usuarios necesita su clave secreta compartida.
  2.- Conociendo la clave de cifrado se puede descifrar fácilmente. La robustez del algoritmo recae en el secreto de la clave.
  3.- Son rápidos y fáciles de implementar.

Criptosistemas asimétricos o de clave pública

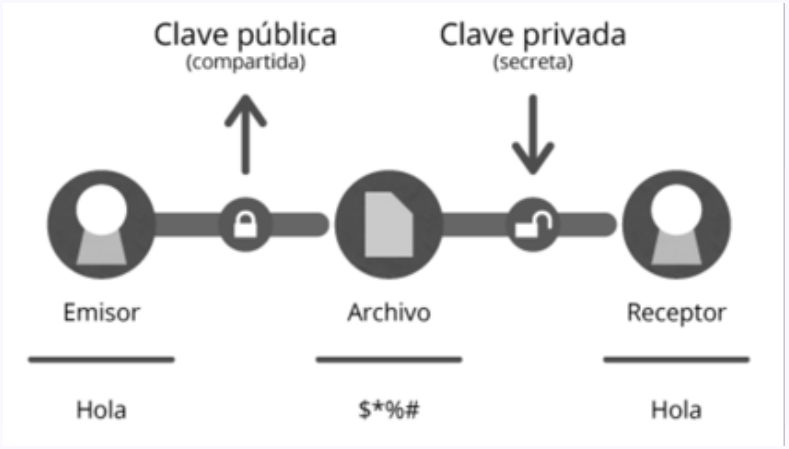


Criptosistemas asimétricos o de clave pública



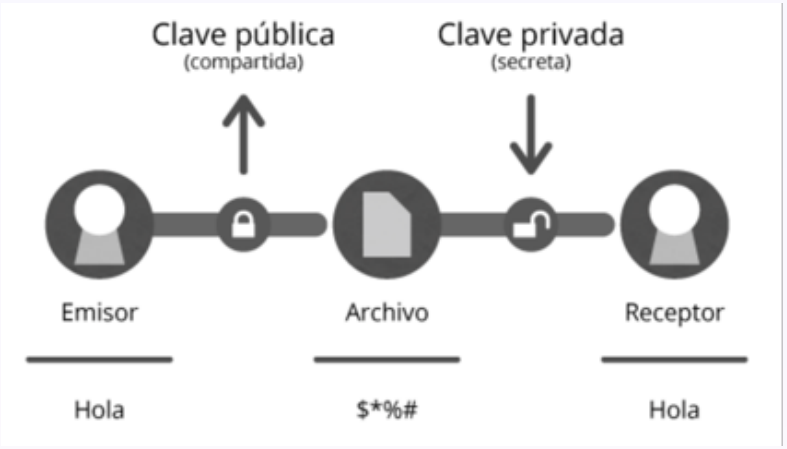
- Introducida por Diffie y Hellman en 1976.

Criptosistemas asimétricos o de clave pública



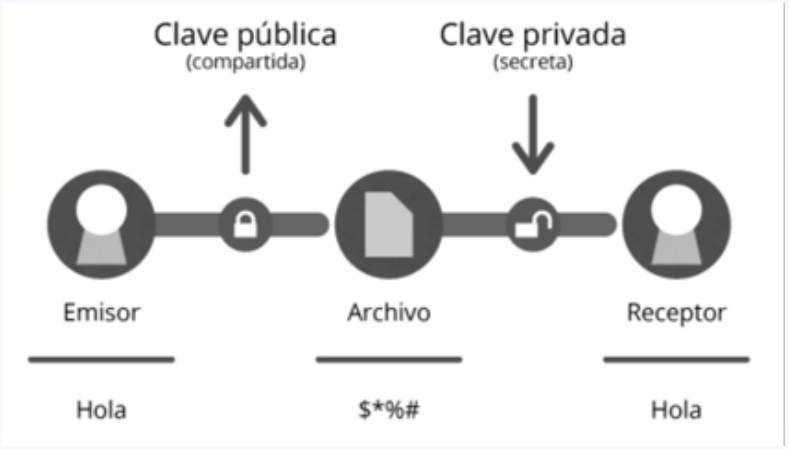
- Introducida por Diffie y Hellman en 1976.
- El emisor y el receptor no necesitan la misma clave. El receptor genera dos claves, una clave pública conocida por todos los interlocutores, y una clave privada sólo conocida por él.

Criptosistemas asimétricos o de clave pública



- Introducida por Diffie y Hellman en 1976.
- El emisor y el receptor no necesitan la misma clave. El receptor genera dos claves, una clave pública conocida por todos los interlocutores, y una clave privada sólo conocida por él.
- La seguridad reside en la dificultad computacional de descubrir la clave privada a partir de la pública.

Criptosistemas asimétricos o de clave pública



- Introducida por Diffie y Hellman en 1976.
- El emisor y el receptor no necesitan la misma clave. El receptor genera dos claves, una clave pública conocida por todos los interlocutores, y una clave privada sólo conocida por él.
- La seguridad reside en la dificultad computacional de descubrir la clave privada a partir de la pública.
- Se usan funciones matemáticas de un sólo sentido o con trampa.

Criptosistemas asimétricos o de clave pública

Principios de la criptografía actual

- Confidencialidad: Sólo los usuarios autorizados tienen acceso a la información. Este principio es el único en el que se basa la criptografía clásica.

Criptosistemas asimétricos o de clave pública

Principios de la criptografía actual

- Confidencialidad: Sólo los usuarios autorizados tienen acceso a la información. Este principio es el único en el que se basa la criptografía clásica.
- Integridad: Garantía de imposibilidad de modificar la información.

Criptosistemas asimétricos o de clave pública

Principios de la criptografía actual

- Confidencialidad: Sólo los usuarios autorizados tienen acceso a la información. Este principio es el único en el que se basa la criptografía clásica.
- Integridad: Garantía de imposibilidad de modificar la información.
- Autenticidad del remitente: Permite verificar que el mensaje recibido fue enviado por el remitente y no por un suplantador.

Criptosistemas asimétricos o de clave pública

Principios de la criptografía actual

- Confidencialidad: Sólo los usuarios autorizados tienen acceso a la información. Este principio es el único en el que se basa la criptografía clásica.
- Integridad: Garantía de imposibilidad de modificar la información.
- Autenticidad del remitente: Permite verificar que el mensaje recibido fue enviado por el remitente y no por un suplantador.
- Autenticidad del destinatario: Permite garantizar la identidad del usuario destinatario.

Criptosistemas asimétricos o de clave pública

Principios de la criptografía actual

- Confidencialidad: Sólo los usuarios autorizados tienen acceso a la información. Este principio es el único en el que se basa la criptografía clásica.
- Integridad: Garantía de imposibilidad de modificar la información.
- Autenticidad del remitente: Permite verificar que el mensaje recibido fue enviado por el remitente y no por un suplantador.
- Autenticidad del destinatario: Permite garantizar la identidad del usuario destinatario.
- No repudio en el origen: Garantía de que el remitente no pueda negar haber enviado dicho mensaje.

Criptosistemas asimétricos o de clave pública

Principios de la criptografía actual

- Confidencialidad: Sólo los usuarios autorizados tienen acceso a la información. Este principio es el único en el que se basa la criptografía clásica.
- Integridad: Garantía de imposibilidad de modificar la información.
- Autenticidad del remitente: Permite verificar que el mensaje recibido fue enviado por el remitente y no por un suplantador.
- Autenticidad del destinatario: Permite garantizar la identidad del usuario destinatario.
- No repudio en el origen: Garantía de que el remitente no pueda negar haber enviado dicho mensaje.
- No repudio en el destino: Garantía de que el destinatario no pueda negar haberlo recibido.

Criptosistemas asimétricos o de clave pública

Principios de la criptografía actual

- Confidencialidad: Sólo los usuarios autorizados tienen acceso a la información. Este principio es el único en el que se basa la criptografía clásica.
- Integridad: Garantía de imposibilidad de modificar la información.
- Autenticidad del remitente: Permite verificar que el mensaje recibido fue enviado por el remitente y no por un suplantador.
- Autenticidad del destinatario: Permite garantizar la identidad del usuario destinatario.
- No repudio en el origen: Garantía de que el remitente no pueda negar haber enviado dicho mensaje.
- No repudio en el destino: Garantía de que el destinatario no pueda negar haberlo recibido.
- Autenticidad de actualidad: Permite verificar que el mensaje es actual, y no un mensaje antiguo reenviado.