

Seguridad y Cifrado

Christian Gimenez

01 Oct 2019

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

Cuento de Alicia y Bob

Erase una vez...

Personajes Típicos

- Alice, Bob, Carol, Dan/Dave, Erin
- Eve, Trudy/Mallory
- Oscar, Faythe

Más: https://es.wikipedia.org/wiki/Alice_y_Bob

Nuestros Personajes

- ¿Quién quiere hacer de Alice? ¿y Bob?
- ¿Quién quiere hacer de Eva y quién de Trudy/Mallory?
- ¿Quién se anima a ser Faythe?

Cuento de Alicia y Bob

Erase una vez...

Personajes Típicos

- Alice, Bob, Carol, Dan/Dave, Erin
- **Eve, Trudy/Mallory**
- Oscar, Faythe

Más: https://es.wikipedia.org/wiki/Alice_y_Bob

Nuestros Personajes

- ¿Quién quiere hacer de Alice? ¿y Bob?
- ¿Quién quiere hacer de Eva y quién de Trudy/Mallory?
- ¿Quién se anima a ser Faythe?

Cuento de Alicia y Bob

Erase una vez...

Personajes Típicos

- Alice, Bob, Carol, Dan/Dave, Erin
- Eve, Trudy/Mallory
- Oscar, Faythe

Más: https://es.wikipedia.org/wiki/Alice_y_Bob

Nuestros Personajes

- ¿Quién quiere hacer de Alice? ¿y Bob?
- ¿Quién quiere hacer de Eva y quién de Trudy/Mallory?
- ¿Quién se anima a ser Faythe?

Cuento de Alicia y Bob

Erase una vez. . .

Personajes Típicos

- Alice, Bob, Carol, Dan/Dave, Erin
- Eve, Trudy/Mallory
- Oscar, Faythe

Más: https://es.wikipedia.org/wiki/Alice_y_Bob

Nuestros Personajes

- ¿Quién quiere hacer de Alice? ¿y Bob?
- ¿Quién quiere hacer de Eva y quién de Trudy/Mallory?
- ¿Quién se anima a ser Faythe?

Cuento de Alicia y Bob

Erase una vez. . .

Personajes Típicos

- Alice, Bob, Carol, Dan/Dave, Erin
- Eve, Trudy/Mallory
- Oscar, Faythe

Más: https://es.wikipedia.org/wiki/Alice_y_Bob

Nuestros Personajes

- ¿Quién quiere hacer de Alice? ¿y Bob?
- ¿Quién quiere hacer de Eva y quién de Trudy/Mallory?
- ¿Quién se anima a ser Faythe?

Cuento de Alicia y Bob

Erase una vez...

Personajes Típicos

- Alice, Bob, Carol, Dan/Dave, Erin
- Eve, Trudy/Mallory
- Oscar, Faythe

Más: https://es.wikipedia.org/wiki/Alice_y_Bob

Nuestros Personajes

- ¿Quién quiere hacer de Alice? ¿y Bob?
- ¿Quién quiere hacer de Eva y quién de Trudy/Mallory?
- ¿Quién se anima a ser Faythe?

Cuento de Alicia y Bob

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

Cuento de Alicia y Bob

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

Cuento de Alicia y Bob

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

Cuento de Alicia y Bob

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

¿Qué Sucede?

- Alice le pide a Faythe que le lleve una carta a Bob
- Eve invita a Faythe a tomar té, le saca la carta y la lee.
- Trudy invita a Faythe a tomar mates, le saca la carta y la cambia.
- Bob recibe la carta y se ofende.

¿Está bien?

- ¿Qué pasaría si fuera información sensible?
 - Dinero
 - Contactos
 - Calendarios y eventos
 - Información privada
 - Etc.
- ¿Cómo se puede solucionar esto?

¿Y si Ciframos?

El cifrado César

Fue usado por Julio César para dar órdenes a sus generales.

¿Cómo funciona?

Nuestra clave es un número (K): la cantidad de letras que desplazar.

Si $K = 1$: desplazamos una letra del abecedario:

Cuando encontramos una de estas letras,

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

La reemplazamos por esta:

B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A

¿Probamos de nuevo?

¡Cifremos con César!

¿Y si Ciframos?

El cifrado César

Fue usado por Julio César para dar órdenes a sus generales.

¿Cómo funciona?

Nuestra clave es un número (K): la cantidad de letras que desplazar.

Si $K = 1$: desplazamos una letra del abecedario:

Cuando encontramos una de estas letras,

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

La reemplazamos por esta:

B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A

¿Probamos de nuevo?

¡Cifremos con César!

¿Y si Ciframos?

El cifrado César

Fue usado por Julio César para dar órdenes a sus generales.

¿Cómo funciona?

Nuestra clave es un número (K): la cantidad de letras que desplazar.

Si $K = 1$: desplazamos una letra del abecedario:

Cuando encontramos una de estas letras,

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

La reemplazamos por esta:

B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A

¿Probamos de nuevo?

¡Cifremos con César!

¿Y si Ciframos?

El cifrado César

Fue usado por Julio César para dar órdenes a sus generales.

¿Cómo funciona?

Nuestra clave es un número (K): la cantidad de letras que desplazar.

Si $K = 1$: desplazamos una letra del abecedario:

Cuando encontramos una de estas letras,

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

La reemplazamos por esta:

B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A

¿Probamos de nuevo?

¡Cifremos con César!

¿Y si Ciframos?

El cifrado César

Fue usado por Julio César para dar órdenes a sus generales.

¿Cómo funciona?

Nuestra clave es un número (K): la cantidad de letras que desplazar.

Si $K = 1$: desplazamos una letra del abecedario:

Cuando encontramos una de estas letras,

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

La reemplazamos por esta:

B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A

¿Probamos de nuevo?

¡Cifremos con César!

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 **Un Poquito de Historia**
 - **Criptografía Clásica**
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 **Un Poquito de Historia**
 - **Criptografía Clásica**
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

¿Sirvió?

- ¿Sirvió a su propósito?
- ¿Sabían el algoritmo? ¿La clave?
 - Principio de Kerckhoff.

Principio de Kerckhoff

- El algoritmo no requiere ser secreto.
- La fuerza del cifrado recae sobre la clave.
- ¿Cuánto tiempo llevó romperlo?
 - Para cuando se rompe el cifrado César ya es tarde.
 - Por eso estudiamos Complejidad computacional.

- ¿Sirvió a su propósito?
- ¿Sabían el algoritmo? ¿La clave?
 - Principio de Kerckhoff.

Principio de Kerckhoff

- El algoritmo no requiere ser secreto.
- La fuerza del cifrado recae sobre la clave.
- ¿Cuánto tiempo llevó romperlo?
 - Para cuando se rompe el cifrado César ya es tarde.
 - Por eso estudiamos Complejidad computacional.

- ¿Sirvió a su propósito?
- ¿Sabían el algoritmo? ¿La clave?
 - Principio de Kerckhoff.

Principio de Kerckhoff

- El algoritmo no requiere ser secreto.
- La fuerza del cifrado recae sobre la clave.
- ¿Cuánto tiempo llevó romperlo?
 - Para cuando se rompe el cifrado César ya es tarde.
 - Por eso estudiamos Complejidad computacional.

- ¿Sirvió a su propósito?
- ¿Sabían el algoritmo? ¿La clave?
 - Principio de Kerckhoff.

Principio de Kerckhoff

- El algoritmo no requiere ser secreto.
- La fuerza del cifrado recae sobre la clave.
- ¿Cuánto tiempo llevó romperlo?
 - Para cuando se rompe el cifrado César ya es tarde.
 - Por eso estudiamos Complejidad computacional.

- ¿Sirvió a su propósito?
- ¿Sabían el algoritmo? ¿La clave?
 - Principio de Kerckhoff.

Principio de Kerckhoff

- El algoritmo no requiere ser secreto.
- **La fuerza del cifrado recae sobre la clave.**
- ¿Cuánto tiempo llevó romperlo?
 - Para cuando se rompe el cifrado César ya es tarde.
 - Por eso estudiamos **Complejidad computacional**.

- ¿Sirvió a su propósito?
- ¿Sabían el algoritmo? ¿La clave?
 - Principio de Kerckhoff.

Principio de Kerckhoff

- El algoritmo no requiere ser secreto.
- **La fuerza del cifrado recae sobre la clave.**
- ¿Cuánto tiempo llevó romperlo?
 - Para cuando se rompe el cifrado César ya es tarde.
 - Por eso estudiamos **Complejidad computacional**.

- ¿Sirvió a su propósito?
- ¿Sabían el algoritmo? ¿La clave?
 - Principio de Kerckhoff.

Principio de Kerckhoff

- El algoritmo no requiere ser secreto.
- **La fuerza del cifrado recae sobre la clave.**
- ¿Cuánto tiempo llevó romperlo?
 - Para cuando se rompe el cifrado César ya es tarde.
 - Por eso estudiamos **Complejidad computacional**.

- ¿Sirvió a su propósito?
- ¿Sabían el algoritmo? ¿La clave?
 - Principio de Kerckhoff.

Principio de Kerckhoff

- El algoritmo no requiere ser secreto.
- **La fuerza del cifrado recae sobre la clave.**
- ¿Cuánto tiempo llevó romperlo?
 - Para cuando se rompe el cifrado César ya es tarde.
 - Por eso estudiamos **Complejidad computacional.**

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

En Nuestro Ejemplo

- Hay 26 posibles claves.
- Una computadora puede computarlas sin problemas.

¡En un segundo!

Usando Algoritmos de Hoy en Día

Supongamos que la contraseña tiene 10 caracteres con:

- Números (10 posibles caracteres)
- Letras mayúsculas (26) y minúsculas (26) en inglés.

¿Cuántas contraseñas posibles?

- $10 + 26 + 26 = 62$ caracteres que podemos usar.
- $VR_m^n = m^n$ es la Variación de m elementos en n posiciones.
- $62^{10} = 8.39299365868 \times 10^{17}$ posibles contraseñas.

Si pensamos que la computadora puede probar 100000 contraseñas por segundo, va a tardar:

- $8.39299365868 \times 10^{17} / 100000 = 8.393 \times 10^{12}$ segundos.
- $8.393 \times 10^{12} / 60 = 1.399 \times 10^{11}$ minutos.
- $1.399 \times 10^{11} / 60 = 2.331 \times 10^9$ horas.
- $2.331 \times 10^9 / 24 = 97141130$ días.
- $97141130 / 360 = 269836$ años!

Pero las contraseñas pueden ser más complejas realmente:

- ¡Pueden tener símbolos, letras de otros idiomas, etc!
- ¡Pueden tener más de 10 caracteres!

Por fuerza bruta se tarda muchísimo aún si usamos un diccionario.

Si pensamos que la computadora puede probar 100000 contraseñas por segundo, va a tardar:

- $8.39299365868 \times 10^{17} / 100000 = 8.393 \times 10^{12}$ segundos.
- $8.393 \times 10^{12} / 60 = 1.399 \times 10^{11}$ minutos.
- $1.399 \times 10^{11} / 60 = 2.331 \times 10^9$ horas.
- $2.331 \times 10^9 / 24 = 97141130$ días.
- $97141130 / 360 = 269836$ años!

Pero las contraseñas pueden ser más complejas realmente:

- ¡Pueden tener símbolos, letras de otros idiomas, etc!
- ¡Pueden tener más de 10 caracteres!

Por fuerza bruta se tarda muchísimo aún si usamos un diccionario.

Si pensamos que la computadora puede probar 100000 contraseñas por segundo, va a tardar:

- $8.39299365868 \times 10^{17} / 100000 = 8.393 \times 10^{12}$ segundos.
- $8.393 \times 10^{12} / 60 = 1.399 \times 10^{11}$ minutos.
- $1.399 \times 10^{11} / 60 = 2.331 \times 10^9$ horas.
- $2.331 \times 10^9 / 24 = 97141130$ días.
- ¡ $97141130 / 360 = 269836$ años!

Pero las contraseñas pueden ser más complejas realmente:

- ¡Pueden tener símbolos, letras de otros idiomas, etc!
- ¡Pueden tener más de 10 caracteres!

Por fuerza bruta se tarda muchísimo aún si usamos un diccionario.

Si pensamos que la computadora puede probar 100000 contraseñas por segundo, va a tardar:

- $8.39299365868 \times 10^{17} / 100000 = 8.393 \times 10^{12}$ segundos.
- $8.393 \times 10^{12} / 60 = 1.399 \times 10^{11}$ minutos.
- $1.399 \times 10^{11} / 60 = 2.331 \times 10^9$ horas.
- $2.331 \times 10^9 / 24 = 97141130$ días.
- ¡ $97141130 / 360 = 269836$ años!

Pero las contraseñas pueden ser más complejas realmente:

- ¡Pueden tener símbolos, letras de otros idiomas, etc!
- ¡Pueden tener más de 10 caracteres!

Por fuerza bruta se tarda muchísimo aún si usamos un diccionario.

Si pensamos que la computadora puede probar 100000 contraseñas por segundo, va a tardar:

- $8.39299365868 \times 10^{17} / 100000 = 8.393 \times 10^{12}$ segundos.
- $8.393 \times 10^{12} / 60 = 1.399 \times 10^{11}$ minutos.
- $1.399 \times 10^{11} / 60 = 2.331 \times 10^9$ horas.
- $2.331 \times 10^9 / 24 = 97141130$ días.
- $97141130 / 360 = 269836$ años!

Pero las contraseñas pueden ser más complejas realmente:

- ¡Pueden tener símbolos, letras de otros idiomas, etc!
- ¡Pueden tener más de 10 caracteres!

Por fuerza bruta se tarda muchísimo aún si usamos un diccionario.

Si pensamos que la computadora puede probar 100000 contraseñas por segundo, va a tardar:

- $8.39299365868 \times 10^{17} / 100000 = 8.393 \times 10^{12}$ segundos.
- $8.393 \times 10^{12} / 60 = 1.399 \times 10^{11}$ minutos.
- $1.399 \times 10^{11} / 60 = 2.331 \times 10^9$ horas.
- $2.331 \times 10^9 / 24 = 97141130$ días.
- $97141130 / 360 = 269836$ años!

Pero las contraseñas pueden ser más complejas realmente:

- ¡Pueden tener símbolos, letras de otros idiomas, etc!
- ¡Pueden tener más de 10 caracteres!

Por fuerza bruta se tarda muchísimo aún si usamos un diccionario.

Si pensamos que la computadora puede probar 100000 contraseñas por segundo, va a tardar:

- $8.39299365868 \times 10^{17} / 100000 = 8.393 \times 10^{12}$ segundos.
- $8.393 \times 10^{12} / 60 = 1.399 \times 10^{11}$ minutos.
- $1.399 \times 10^{11} / 60 = 2.331 \times 10^9$ horas.
- $2.331 \times 10^9 / 24 = 97141130$ días.
- $97141130 / 360 = 269836$ años!

Pero las contraseñas pueden ser más complejas realmente:

- ¡Pueden tener símbolos, letras de otros idiomas, etc!
- ¡Pueden tener más de 10 caracteres!

Por fuerza bruta se tarda muchísimo aún si usamos un diccionario.

Si pensamos que la computadora puede probar 100000 contraseñas por segundo, va a tardar:

- $8.39299365868 \times 10^{17} / 100000 = 8.393 \times 10^{12}$ segundos.
- $8.393 \times 10^{12} / 60 = 1.399 \times 10^{11}$ minutos.
- $1.399 \times 10^{11} / 60 = 2.331 \times 10^9$ horas.
- $2.331 \times 10^9 / 24 = 97141130$ días.
- $97141130 / 360 = 269836$ años!

Pero las contraseñas pueden ser más complejas realmente:

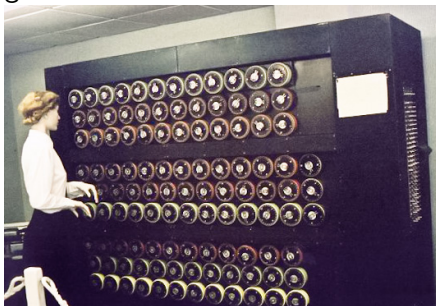
- ¡Pueden tener símbolos, letras de otros idiomas, etc!
- ¡Pueden tener más de 10 caracteres!

Por fuerza bruta se tarda muchísimo aún si usamos un diccionario.

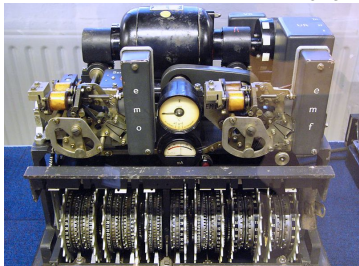
Enigma vs. Bombe



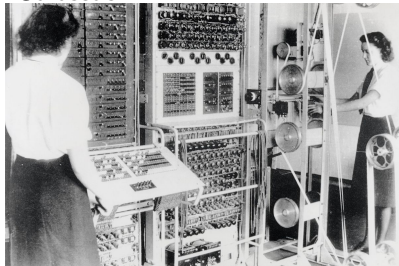
vs.



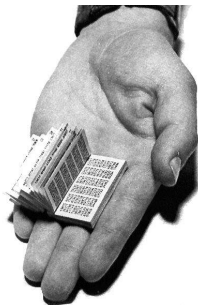
Lorenz vs. Colossus



VS.



OTP vs. Proyecto VENONA



VS



Sip, en Mr. Robot también



Sip, en Mr. Robot También

¿Qué dirá?



Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 **Un Pendrive Perdido**
 - **Se me Cayó un Pendrive**
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes



Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 **Un Pendrive Perdido**
 - **Se me Cayó un Pendrive**
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

Encontramos un Pendrive en la Calle



¿Qué hacemos?

- ¿Qué es lo primero que harían?
- ¿Qué se imaginan que habrá adentro?
 - ¿Datos identificatorios? ¿Curriculum Vitae? ¿Cuentas bancarias?

Encontramos un Pendrive en la Calle



¿Qué hacemos?

- ¿Qué es lo primero que harían?
- ¿Qué se imaginan que habrá adentro?
 - ¿Datos identificatorios? ¿Curriculum Vitae? ¿Cuentas bancarias?

Encontramos un Pendrive en la Calle



¿Qué hacemos?

- ¿Qué es lo primero que harían?
- ¿Qué se imaginan que habrá adentro?
 - ¿Datos identificatorios? ¿Curriculum Vitae? ¿Cuentas bancarias?

Encontramos un Pendrive en la Calle



¿Qué hacemos?

- ¿Qué es lo primero que harían?
- ¿Qué se imaginan que habrá adentro?
 - ¿Datos identificatorios? ¿Curriculum Vitae? ¿Cuentas bancarias?

Encontramos un Pendrive en la Calle



¿Qué hacemos?

- ¿Qué es lo primero que harían?
- ¿Qué se imaginan que habrá adentro?
 - ¿Datos identificatorios? ¿Curriculum Vitae? ¿Cuentas bancarias?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

• ¡A quién se le ocurre dejar las claves en texto plano!

¡Encima esa clase de claves! 1234 ¿En serio?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

• ¡A quién se le ocurre dejar las claves en texto plano!

¡Encima esa clase de claves! 1234 ¿En serio?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

• ¡A quién se le ocurre dejar las claves en texto plano!

¡Encima esa clase de claves! 1234 ¿En serio?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

• ¡A quién se le ocurre dejar las claves en texto plano!

¡Encima esa clase de claves! 1234 ¿En serio?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

• ¡A quién se le ocurre dejar las claves en texto plano!

¡Encima esa clase de claves! 1234 ¿En serio?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

• ¡A quién se le ocurre dejar las claves en texto plano!

¡Encima esa clase de claves! 1234 ¿En serio?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

- ¡A quién se le ocurre dejar las claves en texto plano!

¡Encima esa clase de claves! 1234 ¿En serio?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt Saber de vos

selfieeee.jpg Conocer tu rostro

papa y mama.jpg Saber tu entorno

backup celu/contactos Saber tus contactos

backup celu/calendario Saber tus horarios

yummy.png Tus gustos

claves.txt Las claves de Home-Banking...

- ¡A quién se le ocurre dejar las claves en texto plano!
¡Encima esa clase de claves! 1234 ¿En serio?

Rebobinemos. . .

¿Lo intentamos de nuevo?

¿Y si ciframos los archivos importantes?

Ahora sí, rebobinemos. . .



BACK
TO
THE FUTURE



Rebobinemos. . .

¿Lo intentamos de nuevo?

¿Y si ciframos los archivos importantes?

Ahora sí, rebobinemos. . .



BACK
TO
THE FUTURE



Encontramos un Pendrive en la Calle



¿Qué hacemos?

- ¿Qué es lo primero que harían?
- ¿Qué se imaginan que habrá adentro?
 - ¿Datos identificatorios? ¿Curriculum Vitae? ¿Cuentas bancarias?

Encontramos un Pendrive en la Calle



¿Qué hacemos?

- ¿Qué es lo primero que harían?
- ¿Qué se imaginan que habrá adentro?
 - ¿Datos identificatorios? ¿Curriculum Vitae? ¿Cuentas bancarias?

Encontramos un Pendrive en la Calle



¿Qué hacemos?

- ¿Qué es lo primero que harían?
- ¿Qué se imaginan que habrá adentro?
 - ¿Datos identificatorios? ¿Curriculum Vitae? ¿Cuentas bancarias?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

• ¡Si fuera tan fácil como 1234!

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

• ¡Si fuera tan fácil como 1234!

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

• ¡Si fuera tan fácil como 1234!

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

• ¡Si fuera tan fácil como 1234!

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

• ¡Si fuera tan fácil como 1234!

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

• ¡Si fuera tan fácil como 1234!

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

- ¡Si fuera tan fácil como 1234!

Encontramos un Pendrive en la Calle

Ops, ¡encontré un Pendrive!

¿Qué hago? ¿Y si miramos qué tiene?

(Discusiones éticas acerca de si se debe mirar el contenido o no lo dejamos para más tarde...)

¿Qué podría hacer una persona maliciosa con estos datos?

CV.odt No entiendo.

selfieeee.jpg No puedo ver la imagen.

papa y mama.jpg ¿Quiénes serán?

backup celu/contactos Si supiera el celu de alguno.

backup celu/calendario ¿Tendrá ocupada la tarde?

yummy.png ¿Será una piza o una hamburguesa?

claves.txt Las claves de... ¿?

- ¡Si fuera tan fácil como 1234!

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 **Aplicaciones**
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
Ej.: Se imaginan Home Banking en HTTPS?
- Consolas remotas SSH
Ej.: Se imaginan las consolas de los routers?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
 - No repudio: ¿Lo escribiste realmente vos?
 - No fue alterado: ¿Trudy no cambió el contenido?
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.
 - `juncoma.edu.ar` es realmente de la Universidad!

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
 - No repudio: ¿Lo escribiste realmente vos?
 - No fue alterado: ¿Trudy no cambió el contenido?
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.
 - juncoma.edu.ar es realmente de la Universidad!

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
 - No repudio: ¿Lo escribiste realmente vos?
 - No fue alterado: ¿Trudy no cambió el contenido?
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.
 - `juncoma.edu.ar` es realmente de la Universidad!

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
 - No repudio: ¿Lo escribiste realmente vos?
 - No fue alterado: ¿Trudy no cambió el contenido?
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.
 - `juncoma.edu.ar` es realmente de la Universidad!

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
 - No repudio: ¿Lo escribiste realmente vos?
 - No fue alterado: ¿Trudy no cambió el contenido?
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.
 - `juncoma.edu.ar` es realmente de la Universidad!

Ufff... ¡Muchas!

Computación

- En redes HTTPS, POP3S, SMTPS, etc.
- Sistemas bancarios.
 - ¿Se imaginan Home Banking sin HTTPS?
- Consolas remotas SSH
 - ¿Se imaginan las contraseñas de login y sudo?

DNS y Autenticación

- Con técnicas de cifrado se puede autenticar un mensaje.
 - No repudio: ¿Lo escribiste realmente vos?
 - No fue alterado: ¿Trudy no cambió el contenido?
- Ej.: Paquetes de GNU/Linux se autentican.
- UNComa tuvo que autenticar sus DNS hace un tiempo.
 - juncoma.edu.ar es realmente de la Universidad!

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Periodismo y Hacktivismo

- Edward Snowden y Julian Assange los usaban continuamente.
 - <https://prism-break.org>
- Cifrado de discos y respaldos seguro en caso de que caigan en manos ajenas.
- Chat con OTR (obsoleto ahora se aconseja OMEMO o OpenPGP) para evitar que se filtre información antes de tiempo.
- Mail cifrados.
- Anonimato: TOR, FreeNet, etc. Usan cifrado por computación distribuida.

Criptomonedas

- Se utiliza la criptografía para autenticar transacciones.
- Se firma digitalmente nuevas monedas.
- ¿Para guardar las monedas en tu Wallet?

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini**
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes



Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini**
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

Entonces...

- ¿Sirve el cifrado?
- ¿Lo usan en su día a día?
- ¿Se imaginan qué pueden proteger?
 - ¿Evitaría que le roben datos?
 - ¿Evitaría que se hagan pasar por ustedes (suplantación de identidad)?

Privacidad y datos...

- ¿Es importante su privacidad?
- ¿Se imaginan algún dato de ustedes que no les gustaría que sepa cualquier persona?
- ¿Es importante sus datos personales e identificatorios?

Entonces...

- ¿Sirve el cifrado?
- ¿Lo usan en su día a día?
- ¿Se imaginan qué pueden proteger?
 - ¿Evitaría que le roben datos?
 - ¿Evitaría que se hagan pasar por ustedes (suplantación de identidad)?

Privacidad y datos...

- ¿Es importante su privacidad?
- ¿Se imaginan algún dato de ustedes que no les gustaría que sepa cualquier persona?
- ¿Es importante sus datos personales e identificatorios?

Entonces...

- ¿Sirve el cifrado?
- ¿Lo usan en su día a día?
- ¿Se imaginan qué pueden proteger?
 - ¿Evitaría que le roben datos?
 - ¿Evitaría que se hagan pasar por ustedes (suplantación de identidad)?

Privacidad y datos...

- ¿Es importante su privacidad?
- ¿Se imaginan algún dato de ustedes que no les gustaría que sepa cualquier persona?
- ¿Es importante sus datos personales e identificatorios?

Entonces...

- ¿Sirve el cifrado?
- ¿Lo usan en su día a día?
- ¿Se imaginan qué pueden proteger?
 - ¿Evitaría que le roben datos?
 - ¿Evitaría que se hagan pasar por ustedes (suplantación de identidad)?

Privacidad y datos...

- ¿Es importante su privacidad?
- ¿Se imaginan algún dato de ustedes que no les gustaría que sepa cualquier persona?
- ¿Es importante sus datos personales e identificatorios?

Entonces...

- ¿Sirve el cifrado?
- ¿Lo usan en su día a día?
- ¿Se imaginan qué pueden proteger?
 - ¿Evitaría que le roben datos?
 - ¿Evitaría que se hagan pasar por ustedes (suplantación de identidad)?

Privacidad y datos...

- ¿Es importante su privacidad?
- ¿Se imaginan algún dato de ustedes que no les gustaría que sepa cualquier persona?
- ¿Es importante sus datos personales e identificatorios?

Entonces...

- ¿Sirve el cifrado?
- ¿Lo usan en su día a día?
- ¿Se imaginan qué pueden proteger?
 - ¿Evitaría que le roben datos?
 - ¿Evitaría que se hagan pasar por ustedes (suplantación de identidad)?

Privacidad y datos...

- ¿Es importante su privacidad?
- ¿Se imaginan algún dato de ustedes que no les gustaría que sepa cualquier persona?
- ¿Es importante sus datos personales e identificatorios?

Entonces...

- ¿Sirve el cifrado?
- ¿Lo usan en su día a día?
- ¿Se imaginan qué pueden proteger?
 - ¿Evitaría que le roben datos?
 - ¿Evitaría que se hagan pasar por ustedes (suplantación de identidad)?

Privacidad y datos...

- ¿Es importante su privacidad?
- ¿Se imaginan algún dato de ustedes que no les gustaría que sepa cualquier persona?
- ¿Es importante sus datos personales e identificatorios?

Entonces...

- ¿Sirve el cifrado?
- ¿Lo usan en su día a día?
- ¿Se imaginan qué pueden proteger?
 - ¿Evitaría que le roben datos?
 - ¿Evitaría que se hagan pasar por ustedes (suplantación de identidad)?

Privacidad y datos...

- ¿Es importante su privacidad?
- ¿Se imaginan algún dato de ustedes que no les gustaría que sepa cualquier persona?
- ¿Es importante sus datos personales e identificatorios?



No van a decir, **no tengo nada que ocultar**, ¿no?

- <https://www.eff.org/issues/privacy>
- <https://ssd.eff.org/>
- ¡Hasta en Wikipedia! https://es.wikipedia.org/wiki/Si_no_has_hecho_nada_malo,_no_tienes_nada_que_esconder





No van a decir, **no tengo nada que ocultar**, ¿no?

- <https://www.eff.org/issues/privacy>
- <https://ssd.eff.org/>
- ¡Hasta en Wikipedia! https://es.wikipedia.org/wiki/Si_no_has_hecho_nada_malo,_no_tienes_nada_que_esconder





No van a decir, **no tengo nada que ocultar**, ¿no?

- <https://www.eff.org/issues/privacy>
- <https://ssd.eff.org/>
- ¡Hasta en Wikipedia! https://es.wikipedia.org/wiki/Si_no_has_hecho_nada_malo,_no_tienes_nada_que_esconder





No van a decir, **no tengo nada que ocultar**, ¿no?

- <https://www.eff.org/issues/privacy>
- <https://ssd.eff.org/>
- ¡Hasta en Wikipedia! https://es.wikipedia.org/wiki/Si_no_has_hecho_nada_malo,_no_tienes_nada_que_esconder



Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini**
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes

Para seguir aprendiendo...

- Usar cifrado de clave compartida (simétrico)
- Usar cifrado de clave pública/privada (asimétrico)
- Firmas digitales
- Programas: GnuPG, Kleopatra, etc.
- Utilizar GNU/Linux:
 - Contactarse con @montun (<https://t.me/Montun>)
 - Cifrar el disco de una compu (notebooks) ← @montun

Para seguir aprendiendo...

- Usar cifrado de clave compartida (simétrico)
- Usar cifrado de clave pública/privada (asimétrico)
- Firmas digitales
- Programas: GnuPG, Kleopatra, etc.
- Utilizar GNU/Linux:
 - Contactarse con @montun (<https://t.me/Montun>)
 - Cifrar el disco de una compu (notebooks) ← @montun

Para seguir aprendiendo...

- Usar cifrado de clave compartida (simétrico)
- Usar cifrado de clave pública/privada (asimétrico)
- Firmas digitales
- Programas: GnuPG, Kleopatra, etc.
- Utilizar GNU/Linux:
 - Contactarse con @montun (<https://t.me/Montun>)
 - Cifrar el disco de una compu (notebooks) ← @montun

Para seguir aprendiendo...

- Usar cifrado de clave compartida (simétrico)
- Usar cifrado de clave pública/privada (asimétrico)
- Firmas digitales
- Programas: GnuPG, Kleopatra, etc.
- Utilizar GNU/Linux:
 - Contactarse con @montun (<https://t.me/Montun>)
 - Cifrar el disco de una compu (notebooks) ← @montun

Para seguir aprendiendo...

- Usar cifrado de clave compartida (simétrico)
- Usar cifrado de clave pública/privada (asimétrico)
- Firmas digitales
- Programas: GnuPG, Kleopatra, etc.
- Utilizar GNU/Linux:
 - Contactarse con @montun (<https://t.me/Montun>)
 - Cifrar el disco de una compu (notebooks) ← @montun

Para seguir aprendiendo...

- Usar cifrado de clave compartida (simétrico)
- Usar cifrado de clave pública/privada (asimétrico)
- Firmas digitales
- Programas: GnuPG, Kleopatra, etc.
- Utilizar GNU/Linux:
 - Contactarse con **@montun** (<https://t.me/Montun>)
 - Cifrar el disco de una compu (notebooks) ← **@montun**

Para seguir aprendiendo...

- Usar cifrado de clave compartida (simétrico)
- Usar cifrado de clave pública/privada (asimétrico)
- Firmas digitales
- Programas: GnuPG, Kleopatra, etc.
- Utilizar GNU/Linux:
 - Contactarse con **@montun** (<https://t.me/Montun>)
 - Cifrar el disco de una compu (notebooks) ← **@montun**

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Diaspora, Friendica, Pump.io, Statusnet, Mastodon, etc.
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR
 - XMPP, etc.

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Diaspora, Friendica, Pump.io, Statusnet, Mastodon, etc.
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR
 - XMPP, etc.

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Diaspora, Friendica, Pump.io, Statusnet, Mastodon, etc.
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR
 - XMPP, etc.

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Diaspora, Friendica, Pump.io, Statusnet, Mastodon, etc.
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR
 - XMPP, etc.

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Diaspora, Friendica, Pump.io, Statusnet, Mastodon, etc.
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR
 - XMPP, etc.

¿Seguridad de la Información?

- Hay muchos libros e información
- Hay muchas comunidades interesadas
- Políticas de Seguridad
 - Muchas cosas puede prevenirse ¡sin necesidad de cifrar!
 - A veces basta cambiar algunas costumbres
- Privacidad
 - Redes sociales que respetan tu privacidad:
 - Diaspora, Friendica, Pump.io, Statusnet, Mastodon, etc.
 - Correos cifrados y firmados digitalmente
 - Chats con OMEMO/OTR
 - XMPP, etc.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

Consejos de Última Hora

- Siempre cifren su información sensible
 - Por lo menos, compliquen su acceso.
 - Ej.: Celular con contraseña, contraseña en la sesión de la compu, etc.
- Sería adecuado cifrar los discos de sus notebooks, la memoria del teléfono, etc.
 - ¿Qué pasa si pierdo mi celular?
- Recuerden que las claves pueden romperse, cambiarlas cada tanto.
- Siempre estén prevenidos: TOR, SSH, HTTPS, etc.
- Nunca deben dar **información personal identificatoria** sea parcial o total a desconocidos.
- Nunca deberían aceptar información de importancia si no está firmada digitalmente o que no puedan confirmar su fuente.
- Siempre traten de compartirse claves cuando se encuentren personalmente.

¡Muchas Gracias!



¡Gracias!

¡Gracias por su presencia!

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!**
- 7 Licencia
 - Licencia de Esta Obra
 - Licencia de las Imágenes



Ah, ¿no se terminó?... Ufff, qué cosas... Me quedé sin presentación...



¡Siempre hay algo para charlar!

- TOR, FreeNet, ZeroNet, GNUnet, Bitmessage.
- XMPP + OpenPGP, OMEMO, OTR.
- Redes sociales libres y descentralizadas: Diáspora, Friendica, etc.
- Herramientas: Kleopatra, SSH/STunnel, Cryptsetup y LUKS.
- Criptomonedas y blockchain.
- Criptografía post-quantum.

Ah, ¿no se terminó?... Ufff, qué cosas... Me quedé sin presentación...



¡Siempre hay algo para charlar!

- TOR, FreeNet, ZeroNet, GNUnet, Bitmessage.
- XMPP + OpenPGP, OMEMO, OTR.
- Redes sociales libres y descentralizadas: Diáspora, Friendica, etc.
- Herramientas: Kleopatra, SSH/STunnel, Cryptsetup y LUKS.
- Criptomonedas y blockchain.
- Criptografía post-quantum.

Ah, ¿no se terminó?... Ufff, qué cosas... Me quedé sin presentación...



¡Siempre hay algo para charlar!

- TOR, FreeNet, ZeroNet, GNUnet, Bitmessage.
- XMPP + OpenPGP, OMEMO, OTR.
- Redes sociales libres y descentralizadas: Diáspora, Friendica, etc.
- Herramientas: Kleopatra, SSH/STunnel, Cryptsetup y LUKS.
- Criptomonedas y blockchain.
- Criptografía post-quantum.

Ah, ¿no se terminó?... Ufff, qué cosas... Me quedé sin presentación...



¡Siempre hay algo para charlar!

- TOR, FreeNet, ZeroNet, GNUnet, Bitmessage.
- XMPP + OpenPGP, OMEMO, OTR.
- Redes sociales libres y descentralizadas: Diáspora, Friendica, etc.
- Herramientas: Kleopatra, SSH/STunnel, Cryptsetup y LUKS.
- Criptomonedas y blockchain.
- Criptografía post-quantum.

Ah, ¿no se terminó?... Ufff, qué cosas... Me quedé sin presentación...



¡Siempre hay algo para charlar!

- TOR, FreeNet, ZeroNet, GNUnet, Bitmessage.
- XMPP + OpenPGP, OMEMO, OTR.
- Redes sociales libres y descentralizadas: Diáspora, Friendica, etc.
- Herramientas: Kleopatra, SSH/STunnel, Cryptsetup y LUKS.
- Criptomonedas y blockchain.
- Criptografía post-quantum.

Ah, ¿no se terminó?... Ufff, qué cosas... Me quedé sin presentación...



¡Siempre hay algo para charlar!

- TOR, FreeNet, ZeroNet, GNUnet, Bitmessage.
- XMPP + OpenPGP, OMEMO, OTR.
- Redes sociales libres y descentralizadas: Diáspora, Friendica, etc.
- Herramientas: Kleopatra, SSH/STunnel, Cryptsetup y LUKS.
- Criptomonedas y blockchain.
- Criptografía post-quantum.

Ah, ¿no se terminó?... Ufff, qué cosas... Me quedé sin presentación...



¡Siempre hay algo para charlar!

- TOR, FreeNet, ZeroNet, GNUnet, Bitmessage.
- XMPP + OpenPGP, OMEMO, OTR.
- Redes sociales libres y descentralizadas: Diáspora, Friendica, etc.
- Herramientas: Kleopatra, SSH/STunnel, Cryptsetup y LUKS.
- Criptomonedas y blockchain.
- Criptografía post-quantum.

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 **Licencia**
 - **Licencia de Esta Obra**
 - **Licencia de las Imágenes**



Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 **Licencia**
 - **Licencia de Esta Obra**
 - Licencia de las Imágenes

Excepto en los lugares que se ha indicado lo contrario:

Seguridad y Cifrado se distribuye bajo una Licencia Creative Commons
Atribución-SinDerivadas 4.0 Internacional.



CC-By-ND

Excepto en los lugares que se ha indicado lo contrario:

Esta obra está licenciada bajo la Licencia Creative Commons Atribución-SinDerivadas 4.0 Internacional. Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nd/4.0/>.

Outline

- 1 Cuento de Alicia
 - Cuento de Alicia
- 2 Un Poquito de Historia
 - Criptografía Clásica
- 3 Un Pendrive Perdido
 - Se me Cayó un Pendrive
- 4 Aplicaciones
- 5 C'est Fini
 - Conclusiones
 - ¡Más!
- 6 Ce N'est Pas Fini!
- 7 **Licencia**
 - Licencia de Esta Obra
 - **Licencia de las Imágenes**

- Enigma Machine: <https://commons.wikimedia.org/wiki/File:EnigmaMachine.jpg> bajo la licencia de Dominio Público. Imagen obtenida desde Wikipedia.org.
- Turing Bombe: <https://commons.wikimedia.org/wiki/File:TuringBombeBletchleyPark.jpg> bajo las licencias GNU FDL, CC-By-SA 3.0, CC-By 2.5. Imagen obtenida desde Wikipedia.org.
- Imágenes obtenidas desde Wikipedia.org bajo licencia de Dominio Público: https://en.wikipedia.org/wiki/Lorenz_cipher y https://en.wikipedia.org/wiki/Colossus_computer
- OTP obtenida desde ranum.com (Copyright(C) 1995 Marcus J. Ranum. All rights reserved): http://www.ranum.com/security/computer_security/papers/otp-faq/
- VENONA obtenida desde Wikipedia.org (Imagen de Dominio Público): <https://en.wikipedia.org/wiki/VENONA>

- Tapa de Mr. Robot 2da temporada, obtenida desde IMDB.com (© 1990-2018 IMDb.com, Inc.):
<https://www.imdb.com/title/tt4158110/>
- Imagen obtenida desde GeekWire.com (© 2011-2018 GeekWire, LLC):
<https://www.geekwire.com/2016/mr-robot-rewind-code-cracking-mysterious-mind-bending-epis>
- Pendrive: Obtenida desde Wikimedia commons:
<https://commons.wikimedia.org/wiki/File:SanDisk-Cruzer-USB-4GB-ThumbDrive.jpg> la imagen se encuentra bajo la licencia de Dominio Público.
- Back to the future: obtenida desde Wikimedia commons:
https://commons.wikimedia.org/wiki/File:Back_to_the_Future_film_series_logo.png
- Frase de Freddie Mercury obtenida desde
<https://www.ofrases.com/frase/21979> © ofrases.com.



- Vulcan Hand por qubodup:
<https://openclipart.org/detail/201741/vulcan-hand>
Obtenido desde OpenClipArt y con licencia CC-0.
- Waving man por liftarn:
<https://openclipart.org/detail/181805/waving-man> Obtenido desde OpenClipArt y con licencia CC-0.
- Emojiu1f605 por laughingman11 desde OpenClipart (Licencia: CC-0)
<https://openclipart.org/detail/253500/emojiu1f605>