



Universidad
Carlos III de Madrid

Grupo SeTI · Dpto. Informática

TEMA 2. CRIPTOGRAFÍA

2.1 INTRODUCCIÓN A LOS CRIPTOSISTEMAS

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC LAB

Curso 2016-2017

ÍNDICE

▶ 2.1 Introducción a los criptosistemas

▶ **Criptografía**

- ▶ Definición
- ▶ Modelo de criptosistema
- ▶ Características de los sistemas criptográficos
- ▶ Codificadores vs cifradores

▶ Criptoanálisis

▶ Teoría de la información

- ▶ Entropía
- ▶ Entropía condicionada

▶ Aleatoriedad

▶ Complejidad algorítmica



Definición de criptografía

► Definición clásica (2000 a.c – 1949)

Disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado

► Definición moderna (desde 1976) *Con las guerras.*

Disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado, garantizar su integridad, establecer su autenticidad y prevenir su repudio

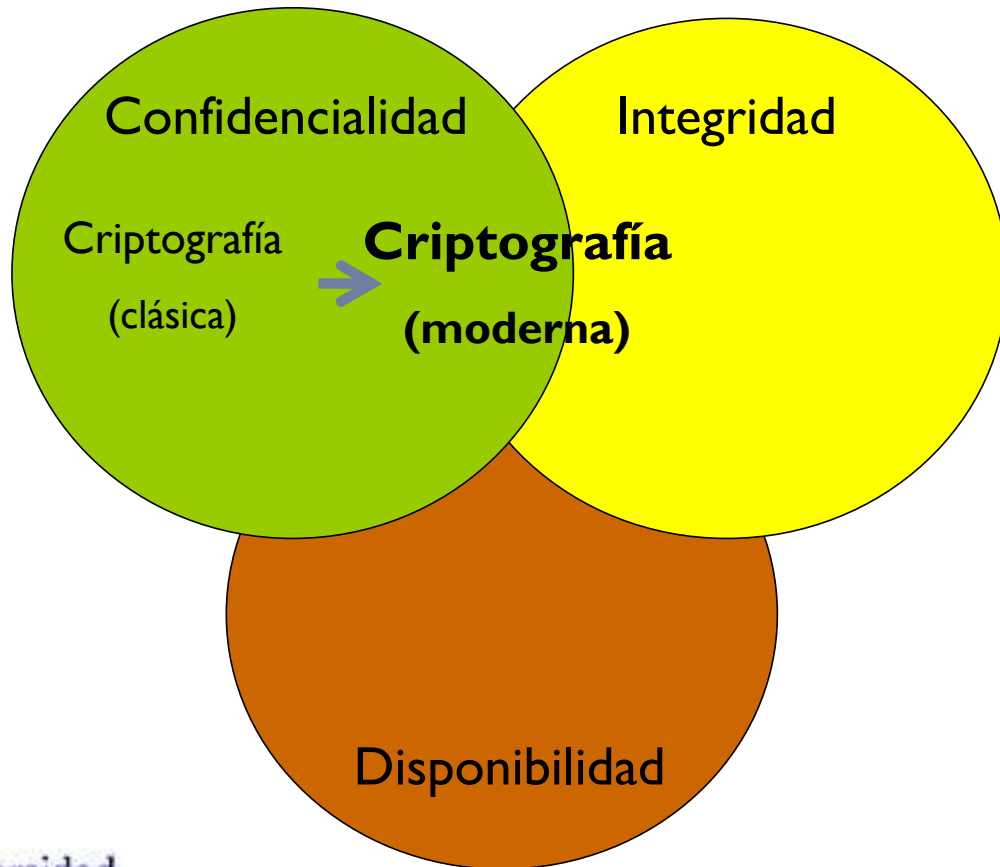
*Lo que no han
sido manipulados*

*Lo Asegurar quien
así es el autor*

*Que no se pueda
negar la autoría,
al tener clave privada
propia*



Definición de criptografía



Modelo de criptosistema

- ▶ Espacio de mensajes : Mensajes originales, sin transformar.

$$M = \{m_1, m_2, \dots\}$$

- ▶ Espacio de cifrados : Mensajes transformados

$$C = \{c_1, c_2, \dots\}$$

- ▶ Espacio de claves : Sirve para configurar el algoritmo de cifrado /descifrado

$$K = \{k_1, k_2, \dots\}$$

- ▶ Familia de transformaciones de cifrado

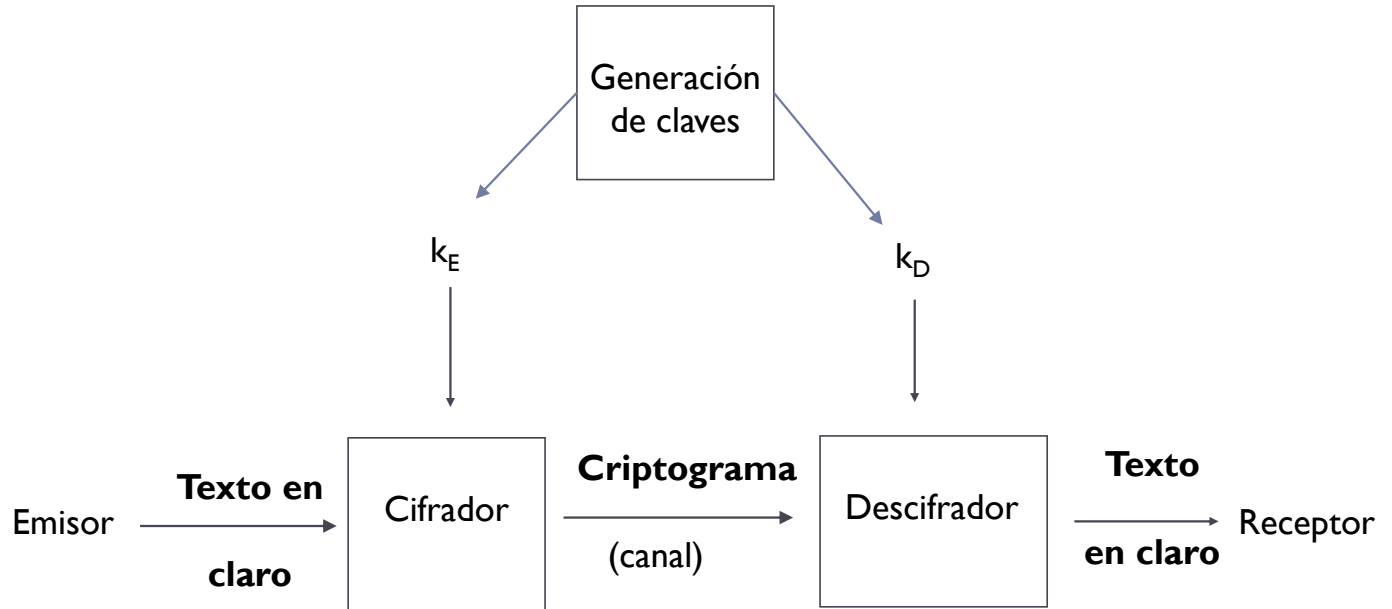
$$E_k : M \rightarrow C$$

- ▶ Familia de transformaciones de descifrado

$$D_k : C \rightarrow M$$



Modelo de criptosistema



k_E y k_D pueden o no ser iguales

Características de los sistemas criptográficos

- ▶ Se caracterizan con tres dimensiones independientes:
 - ▶ Tipo de operaciones realizadas
 - ▶ En general, sustituciones y transposiciones. No puede perderse información. Los más comunes usan el producto de varias ops.
 - ▶ Número de claves usadas
 - ▶ Simétricos o con una clave (también conocido como algoritmos de clave secreta)
 - ▶ Asimétricos o con dos claves (también conocido como algoritmos de clave pública) *Se cifra con la pública, se descifra con la privada.*
 - ▶ Tipo de procesamiento del texto en claro
 - ▶ Por bloques (algoritmos de cifrado en bloque) *grandes trozos.*
 - ▶ Como un flujo continuo de bytes o de bits (algoritmos de cifrado en flujo) *Pequeños trozos*



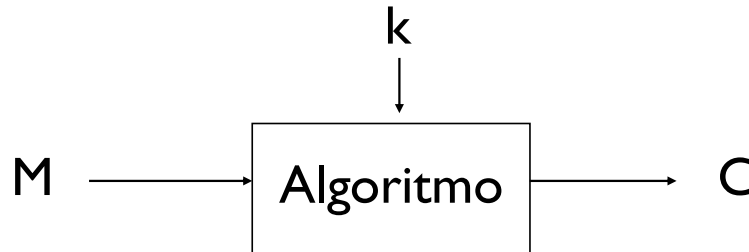
Codificadores vs Cifradores

- **Codificador** : Se sigue una función, que siempre es la misma conocida. Ejen: Morse, ASCII



$$C=f(M)$$

- **Cifrador** : Se sigue un proceso que no es conocido por todos, se necesita una clave. ¿y puede cambiar



$$C=E(k, M)=E_k(M)$$

Codificadores vs Cifradores



ÍNDICE

- ▶ 2.1 Introducción a los criptosistemas
 - ▶ Criptografía
 - ▶ Definición
 - ▶ Modelo de criptosistema
 - ▶ Codificadores vs cifradores
 - ▶ **Criptoanálisis**
 - ▶ Teoría de la información
 - ▶ Entropía
 - ▶ Entropía condicionada
 - ▶ Aleatoriedad
 - ▶ Complejidad algorítmica



Criptografía

- ▶ Ciencia que trata de frustrar las técnicas criptográficas
↳ trata de resolver sin conocer la clave
- ▶ Principio de Kerckhoff

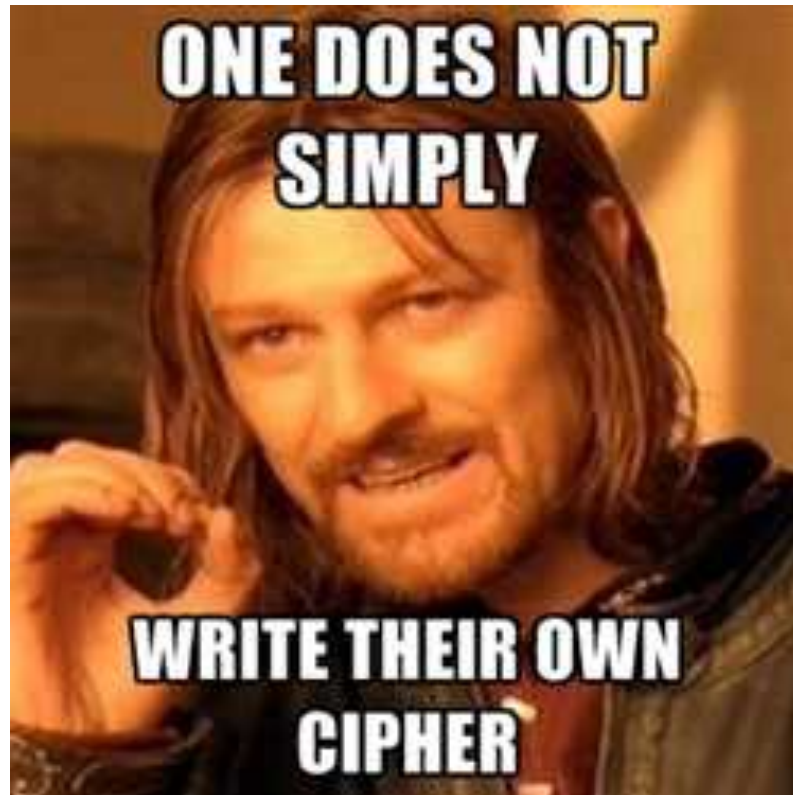
La seguridad del cifrado debe de residir, exclusivamente, en el secreto de la clave

La cryptographie militaire, 1883.
Auguste Kerckhoffs von Nieuwenhof (1835-1903)

- ▶ No a la seguridad por falta de claridad
- ▶ Los ataques se basan en el conocimiento del algoritmo y, quizá, en información adicional sobre el texto en claro



Criptoanálisis



Criptografía

► Objetivo del criptoanalista:

- Principal: Recuperar la clave de descifrado
- Secundario: Descifrar un texto cifrado concreto

¿? Si no
algunos

► Aproximaciones del criptoanalista/atacante:

Ataques al algoritmo

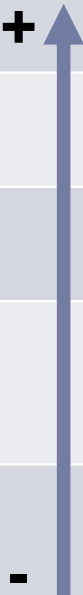


Ataque de fuerza bruta



Criptografía

► Ataques al algoritmo

Ataque	Conocido por el atacante (además de algoritmo)	Dificultad
Texto cifrado	Criptograma	
Texto en claro conocido	Criptograma + uno o más pares (texto en claro, texto cifrado) con la misma clave	
Texto en claro escogido	Criptograma + uno o más pares (texto en claro escogido, texto cifrado) con la misma clave	
Texto cifrado escogido	Criptograma + uno o más criptogramas escogidos por el atacante junto con sus correspondientes textos en claro, con la misma clave	
Texto escogido	Criptograma + uno o más pares (texto en claro escogido, texto cifrado) con la misma clave + uno o más criptogramas escogidos por el atacante junto con sus correspondientes textos en claro, con la misma clave	

Criptografía

- ▶ **Algoritmo de cifrado incondicionalmente seguro**
 - ▶ **No se filtra información** adicional a la conocida por el atacante independientemente de la **longitud del texto cifrado C**
 - con + 2*
 - ▶ **Solo el cifrador de Vernam** es incondicionalmente seguro
 - Es el unico que lo cumple, pero en ciertas condiciones funciona.*
 - Solo quedaria la fuerza bruta*
- ▶ **Algoritmo de cifrado matemáticamente vulnerable**
 - ▶ Si al **aumentar la longitud de C** **se filtra información**
 - se filtra*
 - ▶ **El resto** de algoritmos de cifrado excepto Vernam son matemáticamente vulnerables



Criptografía

Cifrado de Vernam. One-time-pad

- ▶ Cifrado: $E(M) = M \oplus K = m_1 \oplus k_1, m_2 \oplus k_2, \dots, m_n \oplus k_n$

$$\begin{array}{cccccccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ \oplus & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{array}$$

M mensaje ori
 K clave
 C cifrado

- ▶ Descifrado: $M = E(M) \oplus K$

- ▶ Shannon demostró que el cifrado de Vernam es incondicionalmente seguro si la clave K :

- ▶ Es realmente aleatoria
- ▶ Se usa una sola vez

Es de longitud igual o mayor que M

~ Tiene que haber siempre un bit para cada m



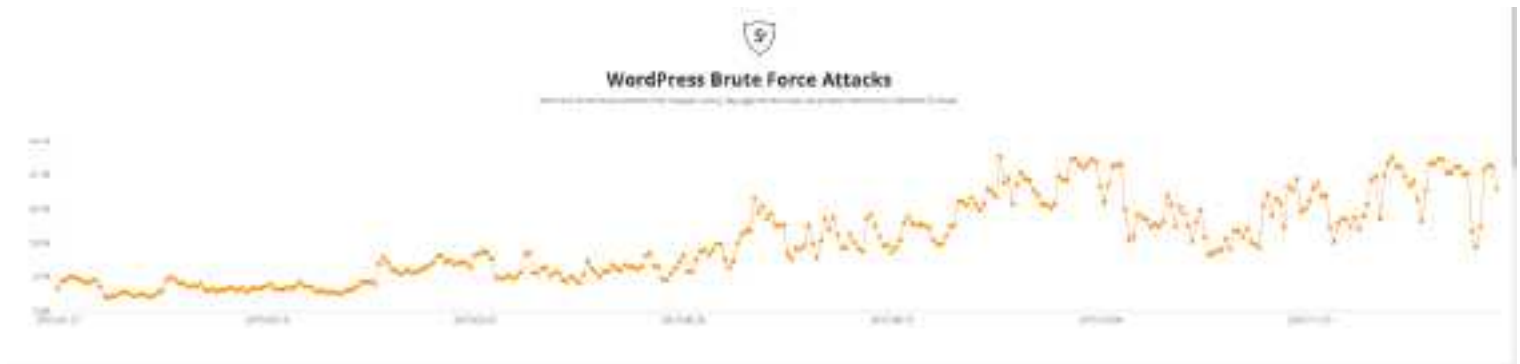
Criptografía

- ▶ Los cifradores incondicionalmente seguros, como Vernam, **NO SON PRÁCTICOS**
- ▶ **Seguridad computacional** (o “No es vulnerable en la práctica”): *Para este cripto análisis se requieren t operaciones y el tiempo en realizarlas es mayor que el tiempo útil. Por lo que ya da igual.*
 - ▶ El criptoanálisis del sistema requiere al menos **t operaciones**
 - ▶ El tiempo de criptoanalizar el algoritmo **excede** el tiempo de vida útil de la información
 - ▶ El **coste de criptoanalizar** el algoritmo **excede** el valor de la información
 - ▶ Para cifradores simétricos
 - ▶ **No existe un algoritmo** capaz de criptoanalizar el cifrador con una **complejidad menor** que la de un **ataque de fuerza bruta**



Criptoanálisis

- ▶ Ataque de fuerza bruta
 - ▶ Probar todas las claves posibles
 - ▶ En media, se deben probar la mitad de las posibilidades para tener éxito

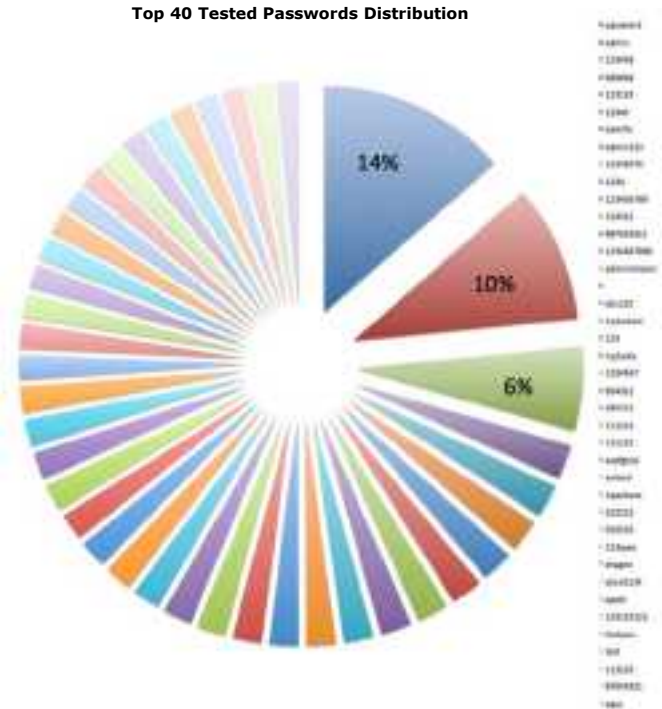
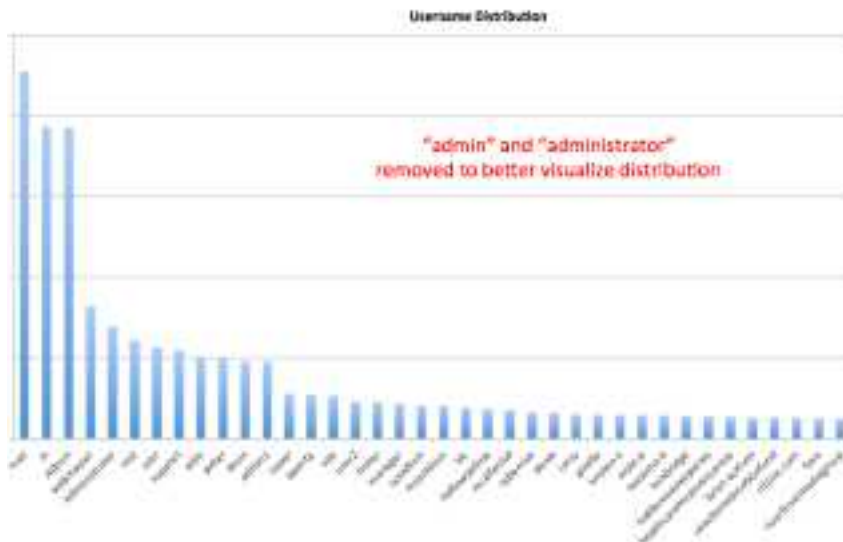


Número de intentos fallidos (Sitios WordPress protegidos por Sucuri)

<https://sucuri.net/security-reports/brute-force/>



► Ataque de fuerza bruta



<https://blog.sucuri.net/2014/03/understanding-denial-of-service-and-brute-force-attacks-wordpress-joomla-drupal-vbulletin.html>

Criptoanálisis

```
File Edit View Terminal Help
[*] 192.168.0.197:3306 MYSQL - [56/72] - Trying username:'ashish1' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [56/72] - failed to login as 'ashish1' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [57/72] - Trying username:'ashish1' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [57/72] - failed to login as 'ashish1' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [58/72] - Trying username:'ashish1' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [58/72] - failed to login as 'ashish1' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [59/72] - Trying username:'gelowo' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [59/72] - failed to login as 'gelowo' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [60/72] - Trying username:'gelowo' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [60/72] - failed to login as 'gelowo' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [61/72] - failed to login as 'gelowo' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [62/72] - Trying username:'gelowo' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [62/72] - failed to login as 'gelowo' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [63/72] - Trying username:'gelowo' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [63/72] - failed to login as 'gelowo' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [64/72] - Trying username:'gelowo' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [64/72] - failed to login as 'gelowo' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [65/72] - Trying username:'gelowo' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [65/72] - failed to login as 'gelowo' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [66/72] - Trying username:'root' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [66/72] - failed to login as 'root' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [67/72] - Trying username:'root' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [67/72] - failed to login as 'root' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [68/72] - Trying username:'root' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [68/72] - failed to login as 'root' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [69/72] - Trying username:'root' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [69/72] - failed to login as 'root' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [70/72] - Trying username:'root' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [70/72] - failed to login as 'root' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [71/72] - Trying username:'root' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [71/72] - failed to login as 'root' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [72/72] - Trying username:'root' with password:'hello'
[*] 192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
```

https://www.youtube.com/watch?v=yixBXV7_qb4



Criptografía

- Tiempo medio requerido para realizar una búsqueda exhaustiva de la clave (ataque de fuerza bruta)

Suposición
razonable

Supuesto
procesamiento
masivo paralelo

Tamaño de la clave (bits)	Número de claves posibles	Tiempo requerido supuesto 1 descifrado/ μ s	Tiempo requerido supuesto 10^6 descifrados/ μ s
32	$2^{32} = 4,3 \cdot 10^9$	$2^{31}\mu s = 35,8$ minutos	2,15 milisegundos
56	$2^{56} = 7,2 \cdot 10^{16}$	$2^{55}\mu s = 1142$ años	10,01 horas
128	$2^{128} = 3,4 \cdot 10^{38}$	$2^{127}\mu s = 5,4 \cdot 10^{24}$ años	$5,4 \cdot 10^{18}$ años
168	$2^{168} = 3,7 \cdot 10^{50}$	$2^{167}\mu s = 5,9 \cdot 10^{36}$ años	$5,9 \cdot 10^{30}$ años
26 caracteres (permutación)	$26! = 4 \cdot 10^{26}$	$2 \cdot 2^{26}\mu s = 6,4 \cdot 10^{12}$ años	$6,4 \cdot 10^6$ años



Criptoanálisis

► Ataque de diccionario

*Es lo primero e
obvio.
Se utiliza cuando se espera
que sean palabras o los
derivados.*

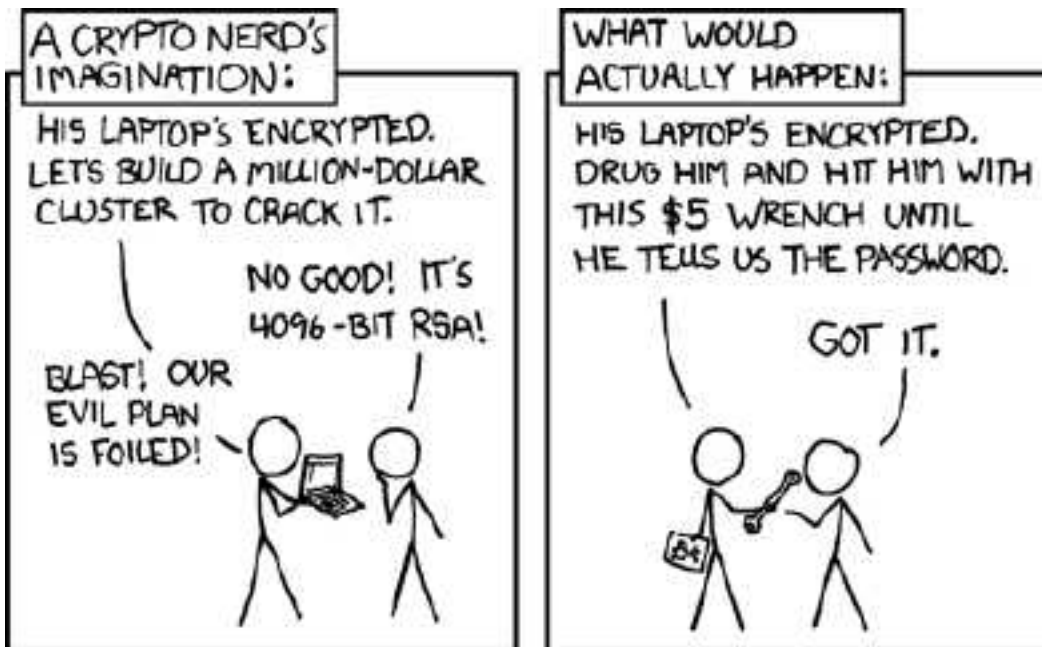
DICTIONARY ATTACK!



Criptoanálisis

Seguridad incondicional vs seguridad computacional vs...

REALIDAD

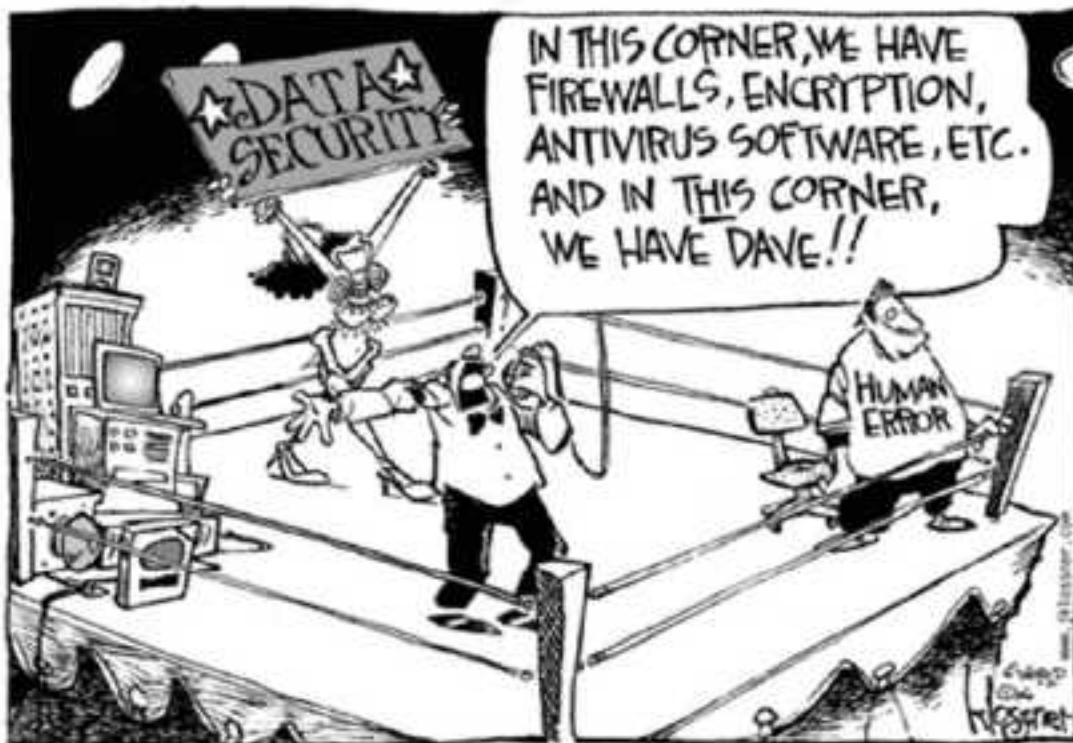


<https://xkcd.com/538/>



Criptoanálisis

- O lo que es peor...



Criptoanálisis



MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS
Arstechnica has arrived in Europe. Check it out!

RISK ASSESSMENT / SECURITY & HACKTIVISM

Hacked French network exposed its own passwords during TV interview

Post-it note on wall revealed network's passwords for YouTube, Instagram

by Sam Mackintosh - Apr 18 2015 12:37 am CEST

Share Tweet Email Print



Way back, David Denis.

While French authorities continued investigating how the TVMonde network had 11 of its stations' signals interrupted the night before, one of its staffers proved just how likely a basic password theft might have led to the incident.

<http://arstechnica.com/security/2015/04/hacked-french-network-exposed-its-own-passwords-during-tv-interview/>



ÍNDICE

- ▶ 2.1 Introducción a los criptosistemas
 - ▶ Criptografía
 - ▶ Definición
 - ▶ Modelo de criptosistema
 - ▶ Características de los sistemas criptográficos
 - ▶ Codificadores vs cifradores
 - ▶ Criptoanálisis
 - ▶ **Teoría de la información**
 - ▶ Entropía
 - ▶ Entropía condicionada
 - ▶ Aleatoriedad
 - ▶ Complejidad algorítmica



TEORÍA DE LA INFORMACIÓN

- ▶ Bases matemáticas. (Claude E. Shannon)
 - ▶ *A mathematical theory of communication*, Bell Syst. Tech. J., vol.23. 1948
- ▶ Fundamentos teóricos de la criptografía: Criptología científica

~
↳ Orígenes
a la era
moderna



TEORÍA DE LA INFORMACIÓN

- ▶ Establece una métrica para evaluar el secreto de un cifrador
- ▶ Se basa en la incertidumbre que sobre el texto en claro tiene un criptoanalista que intercepta un texto cifrado

Visto
antes

- ▶ Cifrador incondicionalmente seguro
 - ▶ No se filtra nada, independientemente de la longitud de C (Vernam)
- ▶ Cifrador matemáticamente vulnerable
 - ▶ Cuanta mayor sea la longitud de C , mayor cantidad de información se filtra (y por tanto está disponible para el criptoanalista)



CANTIDAD DE INFORMACIÓN

- ▶ Sea $M = \{m_1, m_2, \dots, m_n\}$ una **fente** de mensajes estadísticamente **independientes** cuyas probabilidades de ocurrencia respectivas son:

Prob.
 Ocurrencia $\rightarrow p(m_1), \dots, p(m_n)$ con $\sum p(m_i) = 1$

- ▶ La **cantidad de información** (c_i) de un mensaje m_i es:

$$c_i = -\log_2 p(m_i) \text{ bits}$$

invers.

Lo probabilidad de que el mensaje aparezca.

} Un mensaje que se repite aporta menos que uno que es único

- ▶ A mayor $p(m_i)$, menor c_i

Al ser c_i inversa a $p(m_i)$

ENTROPÍA

- ▶ **Entropía** de una fuente M es la cantidad promedio de información transportada por un mensaje perteneciente a dicha fuente

- ▶ **Entropía** de la fuente M :

$$H(M) = - \sum p(m_i) \log_2 p(m_i) \text{ bits}$$

Handwritten annotations:
- A bracket above the formula points to "Cantidad información".
- A bracket below the summation points to "Suma las posibilidades por su cantidad de info".

- ▶ **Bit:** entropía de una fuente con 2 mensajes equiprobables
- $(1/2 \log_2 1/2 + 1/2 \log_2 1/2) = 1/2 \log_2 2 + 1/2 \log_2 2 = 1 \text{ bit}$

ENTROPÍA

- ▶ **Entropía** es la cantidad de información que es previsible ganar tras la aparición de un m_i
- ▶ La **entropía** de M mide la incertidumbre que, a priori, tiene un observador acerca de la aparición de un m_i
- ▶ A mayor entropía, mayor incertidumbre sobre M

Entropía cero = incertidumbre cero = $p(m_i)=1$ para algún i



ENTROPÍA

► Sea $M = \{m_1, m_2, \dots, m_n\}$ con $\sum p(m_i) = 1$

► Propiedades

1. $0 \leq H(M) \leq \log_2 n$ *mínimo si su prob. de aparición es 1 (seguro)*
2. $H(M) = 0$ si y sólo si $p(m_i) = 1$ para algún i
3. $H(M) = \log_2 n$ si y sólo si $p(m_i) = 1/n$ para $1 \leq i \leq n$
↗ máximo solo si son equiprobables

$$\log_2 n = \frac{\log_{10} n}{\log_{10} 2}$$



ENTROPÍA

- ▶ Ej. Considere una fuente con 2 elementos $M=\{m_1, m_2\}$ con $p(m_1)=1/3$ y $p(m_2)=2/3$. Calcule la entropía de M

$$H(M) = - \sum p(m_i) \log_2 p(m_i) = 1/3 \log_2 3 - 2/3 \log_2 2/3 = 0.52 + 0.38 = 0.9$$

- ▶ Ej. Considere una fuente con 2 elementos $M=\{m_1, m_2\}$ con $p(m_1)=0.4$ y $p(m_2)=0.6$. Calcule la entropía de M

$$H(M) = - \sum p(m_i) \log_2 p(m_i) = -0.4 \log_2 0.4 - 0.6 \log_2 0.6 = 0.52 + 0.44 = 0.96$$



ENTROPÍA CONDICIONADA

- ▶ Cuando existe alguna relación entre las apariciones de dos mensajes consecutivos n_j (de una fuente N) y m_i (de una fuente M), la presencia del primero disminuye la incertidumbre del segundo
Conocer el primero me facilita encontrar el segundo, lo reduce mi incertidumbre.
- ▶ La **entropía** de M **condicionada** por N, $H(M|N)$, se define como el valor medio de la cantidad de información de M conocido N

$$H(M|N) = - \sum_j p(n_j) \sum_i p(m_i|n_j) \log_2 p(m_i|n_j)$$

ENTROPÍA CONDICIONADA

- ▶ Ej. $M = \{m_1, m_2, m_3, m_4\}$, $p(m_1) = p(m_2) = p(m_3) = p(m_4) = 1/4$
y $N = \{n_1, n_2\}$, $p(n_1) = p(n_2) = 1/2$.

$N = n_1 \Rightarrow M = m_1 \text{ ó } m_2$ (equiprobablemente)

$N = n_2 \Rightarrow M = m_3 \text{ ó } m_4$ (equiprobablemente)

- ▶ $H(M) = 2$ y
- ▶ $H(M|N) = 1/2(1/2 \lg_2 2 + 1/2 \lg_2 2) + 1/2(1/2 \lg_2 2 + 1/2 \lg_2 2) = 1$
- ▶ El conocimiento de N hace disminuir la entropía resultante de M



ENTROPÍA CONDICIONADA

- ▶ Los métodos criptográficos tratan de maximizar $H(M|N)$ siendo M el conjunto de textos en claro y N el de los cifrados
- ▶ Todos los cifradores (menos Vernan) filtran alguna información sobre el texto en claro al texto cifrado, y según la longitud del texto cifrado crece, mayor es la información filtrada



ÍNDICE

▶ 2.1 Introducción a los criptosistemas

- ▶ Criptografía
 - ▶ Definición
 - ▶ Modelo de criptosistema
 - ▶ Características de los sistemas criptográficos
 - ▶ Codificadores vs cifradores
- ▶ Criptoanálisis
- ▶ Teoría de la información
 - ▶ Entropía
 - ▶ Entropía condicionada

18/62

- ▶ **Aleatoriedad**
- ▶ Complejidad algorítmica



VARIABLE ALEATORIA

- ▶ Sea S un espacio muestral con distribución de probabilidad P (cada posible valor que X puede tomar en S tiene asociada una determinada probabilidad)
- ▶ Una variable aleatoria X es una función de S al conjunto de los números reales $X : S \longrightarrow \mathbb{R}$
- ▶ Ejemplo de variable aleatoria discreta

- ▶ $S = \{\text{cara, cruz}\}$

$$X(s) = \begin{cases} 1 & \text{si } s=\text{cara} \\ 0 & \text{si } s=\text{cruz} \end{cases}$$

- ▶ Si moneda equilibrada: $P(X=1) = 1/2$; $P(X=0) = 1/2$



SECUENCIA ALEATORIA

► Múltiples usos

- Distribución de claves
- Protocolos de autenticación mutua
- Generación de claves de sesión
- Generación de claves para RSA
- Generación de flujos de bits para algoritmos de cifrado simétrico de flujo

► Criterios de aleatoriedad:

- **Distribución uniforme**: La frecuencia de aparición de 1's y 0's debe ser aproximadamente la misma
- **Independencia**: Ninguna subsecuencia puede ser inferida de otras

Se debe comportar de esta manera para no poder deducir el resto de la secuencia.



SECUENCIA ALEATORIA *Analiza la entropía*

► Baterías de tests

- Existen test para probar distribución uniforme

- No existen test para probar independencia *no se puede probar, pero si se puede asegurar que no es independiente.*

- Existen test para demostrar la no independencia

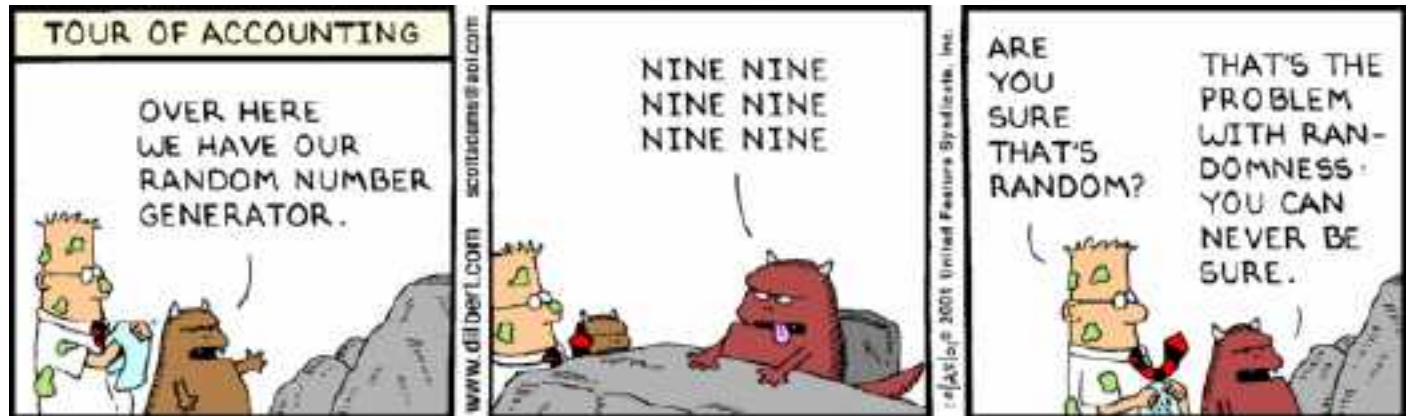
- Si no pasa tests, aleatoriedad descartada

- Si pasa todos los tests, no se puede garantizar aleatoriedad

- El Maurer Universal Test no es definitivo



SECUENCIA ALEATORIA



<http://dilbert.com/strip/2001-10-25>

ALEATORIEDAD

SECUENCIA ALEATORIA

Generadores pseudoaleatorios: pasan las pruebas pero tienen un mecanismo. algoritmo

- ▶ Las aplicaciones criptográficas generalmente utilizan algoritmos para generar números “aleatorios”
- ▶ Aunque una secuencia verdaderamente aleatoria no puede estar generada por un algoritmo dado que éste por definición es determinista
- ▶ Diferencia:
 - ▶ Pseudoaleatoriedad (PRNG)
 - ▶ Algoritmo
 - ▶ Aleatoriedad (TRNG) [Uso de fuentes no deterministas]
 - ▶ Fuente de entropía tomada de ciertos procesos naturales
 - ▶ Eliminación del sesgo con funciones resumen



ÍNDICE

- ▶ 2.1 Introducción a los criptosistemas
 - ▶ Criptografía
 - ▶ Definición
 - ▶ Modelo de criptosistema
 - ▶ Codificadores vs cifradores
 - ▶ Criptoanálisis
 - ▶ Teoría de la información
 - ▶ Entropía
 - ▶ Entropía condicionada
 - ▶ Aleatoriedad
 - ▶ **Complejidad algorítmica**



COMPLEJIDAD ALGORÍTMICA

- ▶ Campo de la matemática que estudia los algoritmos bajo la dificultad de su resolución
- ▶ Clasifica los algoritmos según su complejidad



PROBLEMAS Y ALGORITMOS

► Problema

- Planteamiento de una tarea en un determinado contexto

► Algoritmo

- Conjunto finito de operaciones, que realizadas en un determinado orden, resuelven un problema
- Los algoritmos pueden trabajar sobre un ejemplo particular de problema (problemas particulares)
- Si un algoritmo resuelve todos los problemas particulares
 ⇒ el algoritmo resuelve el problema genérico



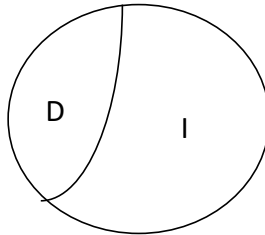
PROBLEMAS Y ALGORITMOS

- ▶ Turing demuestra que no todos los problemas tienen un algoritmo que los resuelva
- ▶ ¡No todos los problemas tienen solución!



PROBLEMAS Y ALGORITMOS

- ▶ Una primera clasificación de los problemas
 - ▶ **Indecidibles (I)**
 - ▶ No resolubles mediante un algoritmo
 - ▶ **Decidibles (D)**
 - ▶ Cuentan con al menos un algoritmo para su resolución

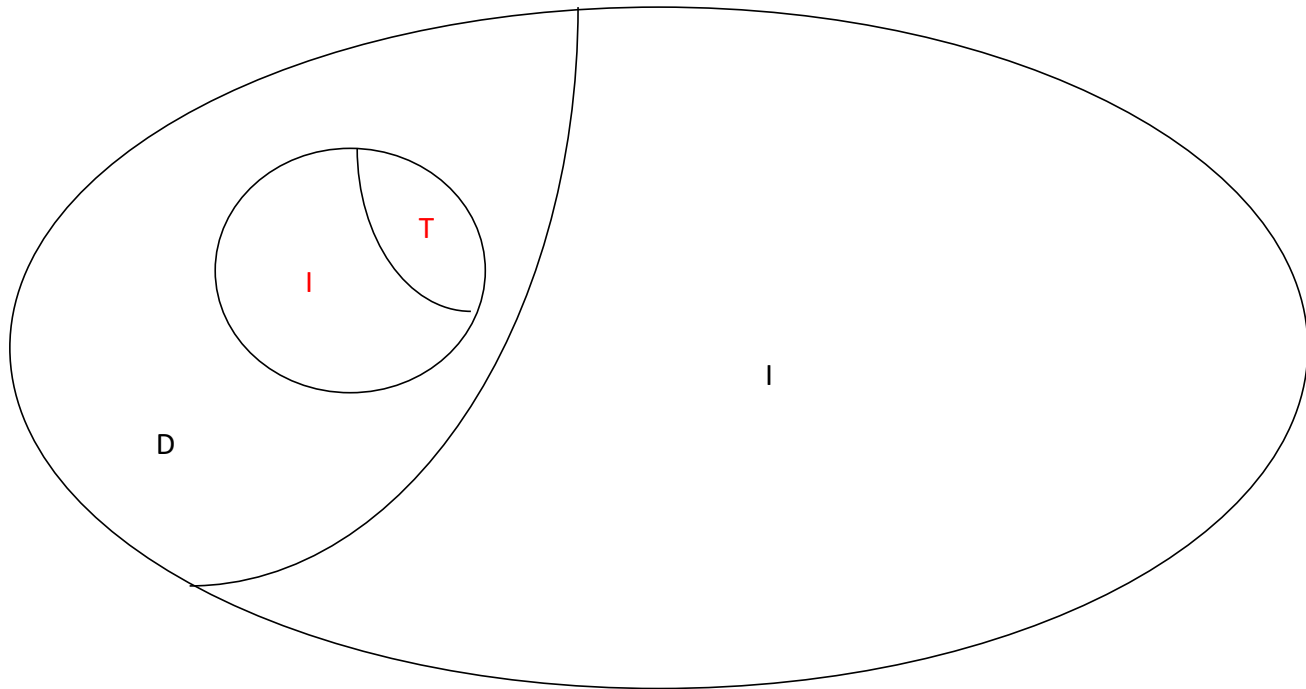


Problemas Tratables e Intratables

- ▶ Existen problemas cuya solución es inabordable por el elevado número de operaciones a realizar
- ▶ Una segunda clasificación de los problemas:
 - ▶ **Intratables (I)**
 - ▶ No es factible obtener su solución en un tiempo razonable con potencia de cálculo actual
 - ▶ **Tratables (T)**
 - ▶ Existen al menos un algoritmo que resuelve cualquier problema particular en tiempo razonable



Problemas Tratables e Intratables



TIEMPO DE EJECUCIÓN

- ▶ La dificultad para resolver una instancia de un problema se mide según su **tiempo de ejecución (t)**
- ▶ Es función del **tamaño de la entrada (n)**
- ▶ Se analiza el comportamiento del algoritmo cuando n crece (comportamiento asintótico)
 - ▶ Se dice que un algoritmo presenta una complejidad **polinómica** si el tiempo t es de orden polinómico o menor
 - ▶ Logarítmico $O(\log n)$: Ej. $t = 5 \log n$ $O(\log n)$
 - ▶ Potencia de n (polinómico) $O(n^c)$: Ej. $t = 2n^3 + 6n$ $O(n^3)$
 - ▶ vs. complejidad **exponencial** si el tiempo t es de orden mayor que polinómico
 - ▶ Exponencial $O(c^n)$: Ej. $t = 3^n + 4n$ $O(3^n)$
 - ▶ Factorial $O(n!)$: Ej. $t = 5n! + 6^n$ $O(n!)$



TIEMPO DE EJECUCIÓN

- ▶ En un ordenador con 1 millón de operaciones por segundo

Tamaño n	$\log_2 n$ (t)	n (t)	n^2 (t)	2^n (t)
10	$3 \cdot 10^{-6}$ s	10^{-5} s	10^{-4} s	10^{-3} s
10^2	$7 \cdot 10^{-6}$ s	10^{-4} s	10^{-2} s	10^{14} siglos
10^3	$10 \cdot 10^{-6}$ s	10^{-3} s	1 s	Muy grande
10^4	$13 \cdot 10^{-6}$ s	10^{-2} s	1,7 min	Muy grande
10^5	$17 \cdot 10^{-6}$ s	10^{-1} s	2,8 h	Muy grande

CLASES DE COMPLEJIDAD ALGORÍTMICA

- ▶ Un problema puede resolverse por distintos algoritmos
- ▶ Los problemas se clasifican en **clases de complejidad** según el tiempo en el que pueden ser resueltos:
 - ▶ **Clase P** (Polynomial time) *polinomial con algoritmo determinista*
 - ▶ **Clase NP** (Non deterministic Polynomial time) *polinomial pero no determinista*
 - ▶ Otras clases...



CLASES DE COMPLEJIDAD ALGORÍTMICA

- ▶ Problemas de **Clase P** (Polynomial time)
 - ▶ Son problemas Tratables
 - ▶ Se resuelven mediante algoritmos polinómicos (buenos algoritmos)
 - ▶ Los algoritmos utilizados son deterministas
 - ▶ En cada paso de computación se determina de forma única el siguiente paso
 - ▶ La concatenación de dos algoritmos P es otro algoritmo **P**



CLASES DE COMPLEJIDAD ALGORÍTMICA

► Problemas de **clase NP** (Non deterministic Polynomial time)

- Contiene problemas Intratables (y tratables)
 - ¿ $P \subset NP$?
- Los problemas intratables se resuelven mediante algoritmos no polinomiales (malos algoritmos), como los exponenciales
- Los algoritmos utilizados son no deterministas
 - En cada paso de computación necesitan una selección entre diferentes opciones
- Ejemplos:

□ Problema del logaritmo discreto → DH, EG

□ Problema de la factorización → RSA ⇒ $e \cdot d \equiv 1 \pmod{\phi(n)}$

Queremos hallar d , pero si es grande x es muy difícil y es NP

$$d = e^{-1} \pmod{\phi(n)}$$
$$d = e^{\phi(n)-1} \pmod{\phi(n)}$$

$n = p \cdot q$ primos $\phi(n) = (p-1)(q-1)$
público e y n
privado d , p y q

