ApuntES de Criptografía

Clase 0

https://apuntes.indcpa.com
Versión 0.0.1, junio 2024

Sobre este curso: objetivo

Objetivo

Demostrar el rol fundamental que *postulados* y *demostraciones* matemáticas juegan en la criptografía moderna, permitiendonos obtener guarantias precisas de seguridad.

- Al final del curso, quiero que tengan las nociones teóricas de base para poder leer sobre protocolos prácticos como SSH y TLS, y entender por que funcionan

Sobre este curso: que

- Vamos a cubrir material fundamental para la comprensión y el diseño de protocolos de cifrado y autenticación
- Este es material "standard", mucho material en ingles disponible:
  1. Katz y Lindell, *Introduction to Modern Cryptography*, Tercera Edicion, CBC Press
  2. Boneh y Shoup, *A Graduate Course in Applied Cryptography*, `https://toc.cryptobook.us`
  3. Rosulek, *The Joy of Cryptography*, `https://joyofcryptography.com`
  4. Smart, *Cryptography, an Introduction*, `https://nigelsmart.github.io/Crypto_Book`
- El análisis criptográfico es una disciplina matemática, pero
- Voy a presentar una selección de resultados que nos permite ver una instancia de cada primitiva útil, pero que tenga la demostración mas simple!

Que es la criptografía

Que es la criptografía

La criptografía es la ciencia/el arte de "proteger" información, en transito y en reposo.

Seguridad de la información: la tríade "CIA"

- **C**onfidencialidad: solamente las partes "autorizadas" pueden leer los datos
- **I**ntegridad: las partes "autorizadas" pueden averiguar que un dato no fue modificado
- **A**utenticidad: las partes "autorizadas" pueden verificar el origen de un dato

Que no puede garantizar:

- "**A**vailability": la criptografía en si no puede proteger un servidor de un ataque "denial of service"

Que no es:

- La criptografía no es *esteganografía*, o sea el estudio de como *ocultar* información confidencial dentro de mensajes no confidenciales. En criptografía, nada es "ocultado".

Glosario

Esquema, protocolo, primitiva, control

Mucha terminología tiene definición borrosa. Generalmente,

- Un *esquema* es un conjunto de algoritmos que otorgan un determinado tipo de protección. Cada algoritmo corre en un particular sistema.
- Un *protocolo* es una descripción de operaciones entre múltiples partes, para otorgar comunicación segura. Varios esquemas pueden ser utilizados.
- Una *primitiva* es un esquema o sub-componente de un esquema que se lo ve como componente "atomica" de un sistema mas grande.
- Un *control* es un "componente" en un sistema "de seguridad": *e.g.*, cerraduras, matafuegos, sistemas de firma digital, antivirus, leyes de protección de datos.

Glosario

Criptografía, criptoanálisis, criptología

- La criptografia es el estudio de como construir "controles de seguridad" de datos
- La criptoanálisis es el estudio de los ataques a controles criptográficos
- La criptología es $\{\text{criptografia}\} \cup \{\text{criptanalisis}\}$

Es común que "criptografia" se use en lugar de "criptologia".

Historia

- Históricamente, la criptografía es una disciplina bélica.
- Un ejemplo clásico: el "cifrado de Cesar"

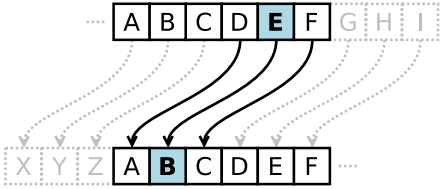
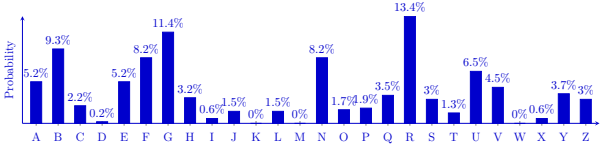


Figure 1: El "cifrario de Cesar" con "clave" = 3.

- Por mucho tiempo, los cifrados utilizaban técnicas parecidas.
- En 1553, Bellaso describe un cifrado luego atribuido a Vigenère, que utiliza una palabra clave que determina múltiples cifrado de Cesar. Este fue el estado del arte hasta 1863.

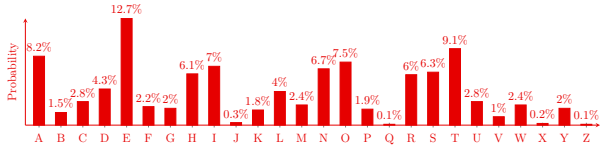
Estos tipos de cifrado son triviales de atacar usando "análisis de frecuencia".

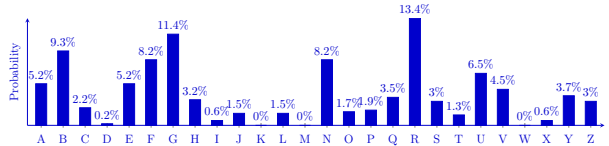
GB OR, BE ABG GB OR, GUNG VF GUR DHRFGVBA:
JURGURE 'GVF ABOYRE VA GUR ZVAQ GB FHSSRE
GUR FYVATF NAQ NEEBJF BS BHGENTRBHF SBEGHAR,
BE GB GNXR NEZF NTNVAFG N FRN BS GEBHOYRF,
NAQ OL BCCBFVAT RAQ GURZ? GB QVR—GB FYRRC,
AB ZBER; NAQ OL N FYRRC GB FNL JR RAQ
GUR URNEG-NPUR, NAQ GUR GUBHFNAQ ANGHENY FUBPXF
GUNG SYRFU VF URVE GB: 'GVF N PBAFHZZNGVBA
QRIBHGYL GB OR JVFU'Q. GB QVR, GB FYRRC.
GB FYRRC, CREPUNAPR GB QERNZ—NL, GURER'F GUR EHO,
SBE VA GUNG FYRRC BS QRNGU JUNG QERNZF ZNL PBZR,
JURA JR UNIR FUHSSYRQ BSS GUVF ZBEGNY PBVY,
ZHFG TVIR HF CNHFR. GURER'F GUR ERFCRPG
GUNG ZNXRF PNYNZVGL BS FB YBAT YVSR.



Estos tipos de cifrado son triviales de atacar usando "análisis de frecuencia".

TO BE, OR NOT TO BE, THAT IS THE QUESTION:
WHETHER 'TIS NOBLER IN THE MIND TO SUFFER
THE SLINGS AND ARROWS OF OUTRAGEOUS FORTUNE,
OR TO TAKE ARMS AGAINST A SEA OF TROUBLES,
AND BY OPPOSING END THEM? TO DIE—TO SLEEP,
NO MORE; AND BY A SLEEP TO SAY WE END
THE HEART-ACHE, AND THE THOUSAND NATURAL SHOCKS
THAT FLESH IS HEIR TO: 'TIS A CONSUMMATION
DEVOUTLY TO BE WISH'D. TO DIE, TO SLEEP.
TO SLEEP, PERCHANCE TO DREAM—AY, THERE'S THE RUB,
FOR IN THAT SLEEP OF DEATH WHAT DREAMS MAY COME,
WHEN WE HAVE SHUFFLED OFF THIS MORTAL COIL,
MUST GIVE US PAUSE. THERE'S THE RESPECT
THAT MAKES CALAMITY OF SO LONG LIFE.





- La criptografía de este periodo era mayormente un arte
- (Si quieren aprender mas de sistemas de cifrado historicos, vean los capitulos 3 y 4 de "Smart")
- No había definiciones precisas de seguridad, o garantías matemáticas de seguridad
- También se dependía mucho de mantener secretos los controles de seguridad

El principio de Kerckhoffs

La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
Hoy diríamos: *la seguridad de un sistema de cifrado debe solo depender en que las claves usadas sean secretas, no los detalles del sistema.*

El estudio académico (públicamente disponible) de criptografía empieza después de WWII:

- 1949, Shannon publica *Communication Theory of Secrecy Systems*, trabajando par Bell Labs
- 1973, Feistel y Coppersmith diseñan el primer cifrario "de Feistel" desde IBM
- 1976, un cifrario de Feistel viene usado para definir el estandar DES
- 1976, Diffie y Hellman publican *New Directions in Cryptography*
- 1977, Rivest Shamir y Adleman publican el cifrario de clave publica RSA
- 1982, Goldwasser y Micali definen la noción de *seguridad semántica*
- 1986, Goldreich, Goldwasser y Micali definen la noción de *función pseudoaleatoria*
- 1988, Luby y Rackoff demuestran el diseño de Feistel seguro

Solo gracias a las nociones de seguridad desarrolladas en los 80, la criptografía se vuelve propiamente una ciencia.

Los diseños de los esquemas se vuelven mas complicados y "matematicos", también gracias a la capacidad de calculo de las computadoras.

Hoy en día, la criptografía ve amplio uso civil,

- En sistemas de pago electrónico,
- En sistemas de privacidad online,
- En sistemas de almacenamiento seguro de datos.

La mas común taxonomía etiqueta los esquemas criptográficos en sistemas *de clave secreta/privada* (o *criptografía simétrica*), y *de clave publica* (o *criptografía asimétrica*).

Nosotros vamos a cubrir ambas componentes, empezando por la simétrica, y siguiendo por la asimétrica.

Mapa de los contenidos