

CRIPTOLOGÍA

A PARTIR DE AHORA VEREMOS UNA CODIFICACIÓN DONDE EL OBJETIVO ES EL GARANTIZAR EL SECRETO O PRIVACIDAD DE LOS MENSAJES, DE MANERA QUE SOLO LA PERSONA A LA QUE SON ENVIADOS, SU RECEPTOR LEGAL, PUEDA CONOCERLOS.

SI EL CANAL DE TRANSMISIÓN EMPLEADO ES INSEGURO, ES DECIR SUSCEPTIBLE DE SER INTERVENIDO O ESPIADO POR TERCERAS PERSONAS, LA SOLUCIÓN ES DISFRAZAR EL MENSAJE MEDIANTE UN CÓDIGO SECRETO.

LA CRIPTOLOGÍA ES LA CIENCIA QUE ESTUDIA LOS CRIPTOSISTEMAS (O SISTEMAS CRIPTOGRÁFICOS O CÓDIGOS SECRETOS)

DENTRO DE ELLA HAY DOS PARTES

- CRIPTOGRAFÍA: DISEÑO E IMPLEMENTACIÓN DE LOS CRIPTOSISTEMAS
- CRIPTANÁLISIS: QUE TRATA DE ROMPERLOS

LA CRIPTOLOGÍA TIENE UNA HISTORIA MILENARIA, PERO SÓLO DESDE LOS 70'S PASA DE SER UN CONJUNTO DE REGLAS EMPÍRICAS ("TRUQUITOS") A SER UNA CIENCIA.

ES UNA DISCIPLINA QUE NO PARA DE CRECER Y QUE IMPULSA EL DESARROLLO DE OTROS CAMPOS MATEMÁTICOS

HISTÓRICAMENTE LA CRIPTOGRAFIA ESTÁ LIGADA A LA NECESIDAD DE MANTENER SECRETAS COMUNICACIONES ENTRE GOBIERNOS Y/O MILITARES. EJ: MÁQUINA ENIGMA

YA NO ES ALGO PROPIO DE GOBIERNOS, MILITARES O GRANDES COMPAÑÍAS. AHORA SE USA PARA PROTEGER DATOS PERSONALES, CONTROL DE ACCESO (BANCOS, TARJETAS CRÉDITO), FIRMA DIGITAL, ...

ALGUNOS EJEMPLOS USO CRIPTOGRAFIA

PROTODCOLOS AUTENTIFICACIÓN

-AUTENTIFICACIÓN DE MENSAJE: GARANTIZA MENSAJE NO HA SIDO ALTERADO

-AUTENTIFICACIÓN USUARIO:

- FIRMA DIGITAL

- DESAFIO RESPUESTA: USUARIO DEMUESTRA TENER UNA
PIEZA SECRETA DE INFORMACIÓN

← PASSWORD USUARIO

PROTODCOLOS COMPARTIR SECRETOS

PRUEBAS CONOCIMIENTO CERO: CONVENCER A OTRO DE QUE SE
POSEE CIERTA INFORMACIÓN SIN REVELARLA

TRANSACCIONES ELECTRÓNICAS SEGURAS

ELECCIONES ELECTRÓNICAS

COMPUTACIÓN MULTI-PARTE



EVE CRIPTOANALISTA (Ó ENEMIGO)

EVE QUIERE INFERIR PROCESO COMUNICACIÓN:

- QUIERE CONOCER CONTENIDO COMUNICACIÓN
- SOPLANTAR PERSONALIDAD
- MODIFICAR MENSAJE
- OTROS FINES MALÉVOLS

LA CRIPTOGRAFÍA PROPORCIONA MÉTODOS PARA QUE UN CANAL INSEGURO SE CONVIERTA EN UN CANAL EN EL QUE SE PUEDA CONFIAR.

CRIPTOANÁLISIS: BUSCA ROMPER LA SEGURIDAD

INGREDIENTES DE UN CRIPTOSISTEMA:

- CONJUNTO \mathcal{M} , CONJUNTO DE MENSAJES ORIGINALES O MENSAJES EN CLARO. NORMALMENTE $\mathcal{M} = A^*$, ES DECIR LOS MENSAJES $M \in \mathcal{M}$ SON SUCESSIONES FINITAS DE SÍMBOLOS DE UN CIERTO ALFABETO
- CONJUNTO FINITO K , LLAMADO CONJUNTO DE CLAVES O LLAVES
- CONJUNTO DE MENSAJES CIFRADOS \mathcal{C} , NORMALMENTE $\mathcal{C} = A^*$
- APLICACIÓN DE CIFRADO O ENCRIPCIÓN

$$c: \mathcal{M} \times K \rightarrow \mathcal{C}$$

- UNA APLICACIÓN DE DESCIFRADO

$$d: \mathcal{C} \times K \rightarrow \mathcal{M}$$

- UN CONJUNTO DE NODOS O USUARIOS N JUNTO CON UN SUBCONJUNTO $L \subset N \times N$, LLAMADO CONJUNTO DE LÍNEAS DE TRANSMISIÓN.

UN ELEMENTO DE L ES $(e, r) \in N \times N$, DONDE e ES EL EMISOR Y r EL RECEPTOR

- PARA CADA LÍNEA $\ell = (e, r) \in L$, UNA CLAVE $k_\ell \in K$ DE CIFRADO Y UNA CLAVE $k'_\ell \in K$ DE DESCIFRADO TALES QUE

$$d(c(M, k_\ell), k'_\ell) = M$$

• PARA ENVIAR e UN MENSAJE A r , CON $\ell = (e, r) \in L$ e CIFRA EL MENSAJE CALCULANDO: $c(M, k_\ell) \in \mathcal{C}$

• EL NODO r RECUPERA EL MENSAJE EN CLARO CALCULANDO

$$d(c(M, k_\ell), k'_\ell) = M$$

CLAVE PRIVADA Y PÚBLICA

- CLAVE PRIVADA: TODOS SISTEMAS CRIPTOGRÁFICOS CLÁSICOS
- CLAVE PÚBLICA: APARECEN 70'S CON LA IMPLANTACIÓN TELECOMUNICACIONES E INFORMÁTICA

CLAVE PRIVADA

LOS USUARIOS DEL SISTEMA, NORMALMENTE POCOS E IDEALMENTE DOS, COMPARTEN Y GUARDAN EN SECRETO UNA PAREJA DE CLAVES DE CIFRADO Y DESCIFRADO (K, K') .

NORMALMENTE SI CONOCES K PUEDES CALCULAR FÁCILMENTE K' (Y VICEVERSA)

CIFRADO Y DESCIFRADO

$$d(c(m, K), K') = m$$

PARA CUALQUIER MENSAJE EN CLARO m

COMO EL CÁLCULO DE UNA CLAVE A PARTIR DE
OTRA ES SENCILLO, NO SUPONE PÉRDIDA GENERALI-
DAD SUPONER QUE SE TRATA DE LA MISMA CLAVE
 $K=K'$. Y POR ESO ESTOS SISTEMAS SE LLAMAN
DE CLAVE PRIVADA O SIMÉTRICOS

LA CLAVE K ES CONOCIDA POR ALICE Y BOB
Y DEBE PERMANECER SECRETA PARA LOS DEMÁS.
DE MANERA QUE AUNQUE EVE INTERCEPTE EL
MENSAJE $C(M, K)$ Y CONOZCA LAS APLICACIO-
NES DE CIFRADO Y DESCIFRADO, NO PUEDA
RECUPERAR M

CLAVE PÚBLICA Ó ASIMÉTRICA

$L = N \times N$ Y CADA USUARIO u DEL SISTEMA TIENE UN PAR DE CLAVES (e_u, d_u)

- e_u ES PÚBLICA, Y ES LA QUE USA CUALQUIER OTRO USUARIO DEL SISTEMA PARA ENVIAR UN MENSAJE CIFRADO A u .
- d_u ES SÓLO CONOCIDA POR EL USUARIO u Y ES LA QUE USA PARA DESCIFRAR LOS MENSAJES QUE RECIBE

LAS CLAVES USADAS EN LA LÍNEA $l = (a, b)$ SON LAS DEL USUARIO b , $k_e = e_b$ Y $k_e' = d_a$.

CONDICIÓN:

AÚN CONOCIDA e_u SEA IMPOSIBLE EN LA PRÁCTICA
EL CÁLCULO DE LA CLAVE PRIVADA d_u

ESTO SE INTERPRETA EN TÉRMINOS DE COMPLEJIDAD
COMPUTACIONAL DEL CÁLCULO DE d_u A PARTIR DE e_u
Y DE LA CANTIDAD DE PARES DE MENSAJES
EN CLARO Y CIFRADO QUE TENGA EL CRIPTOANAL-
LISTA.

CONDICIONES DIFFIE-HELLMAN:

(DE 1976, ANTES DE CONOCER NINGÚN EJEMPLO)

- CÁLCULO CLAVES PÚBLICA Y PRIVADA DEBE SER COMPUTACIONALMENTE SENCILLO
- PROCESO CIFRADO DEBE SER COMPUTACIONALMENTE SENCILLO
- PROCESO DESCIFRADO, CONOCIENDO LA CLAVE PRIVADA, DEBE SER COMPUTACIONALMENTE SENCILLO
- OBTENER CLAVE PRIVADA A PARTIR DE LA PÚBLICA, DEBE SER UN PROBLEMA "COMPUTACIONALMENTE IMPOSIBLE"
- OBTENER MENSAJE EN CLARO, CONOCIDO EL MENSAJE CIFRADO Y LA CLAVE PÚBLICA, DEBE SER COMPUTACIONALMENTE IMPOSIBLE.

CRIPTOANALISIS

OBJETIVO ES DESCUBRIR CONTENIDO MENSAJE CIFRADO , Y A
SER POSIBLE MÉTODO Y CLAVE UTILIZADA

TAMBIÉN PUEDE INTERFERIR E INTERVENIR EL SISTEMA
DE COMUNICACIÓN FALSEANDO MENSAJES E IDENTIDADES

ANTIGUAMENTE , SE PODIA MANTENER SECRETO EL SISTEMA
DE CIFRADO . AHORA NO ES POSIBLE , SE NECESITAN
MÉTOS ESTANDARIZADOS Y POR TANTO CONOCIDOS
ADEMÁS SE QUIERE "VENDER" LA SEGURIDAD.

TIPOS DE ATAQUES

A) ATAQUES PASIVOS

A PARTIR DE UN TEXTO CIFRADO T INTENTA DESCUBRIR EL MENSAJE EN CLARO M . Y A SER POSIBLE DE LA CLAVE DE CIFRADO. TIPOS:

- TEXTO CIFRADO CONOCIDO: SE CONOCE SÓLO T
- TEXTO CLARO CONOCIDO: SE CONOCE UNA PARTE DE M Y T
- TEXTO CLARO ELECIDO: CRIPTOANALISTA PUEDE ELEGIR UN TEXTO EN CLARO Y CONOCER SU CIFRADO

B) ATAQUES ACTIVOS:

CRIPTOANALISTA INTENTA

- SUSTITUIR PERSONALIDAD USUARIOS
- FALSEAR MENSAJES

SEGURIDAD

- **SEGURIDAD PERFECTA**: ES IRROMPIBLE AUN CUANDO EL CRIPTRANALISTA TIENE TIEMPO Y RECURSOS ILIMITADOS
EJ: VERNAM Y BB84 (CANAL CUÁNTICO)
- **SEGURIDAD CONDICIONAL**: ES SEGURO HASTA QUE SE DESARROLLEN NUEVOS O MEJORES MÉTODOS
- **SEGURIDAD PROBABLE**: SISTEMAS QUE NO SE HAN ROTO PERO NO PODEMOS DEMOSTRAR MATEMÁTICAMENTE SU SEGURIDAD. EJ: AES
- **SEGURIDAD COMPUTACIONAL**: SISTEMAS BASADOS EN LA COMPLEJIDAD COMPUTACIONAL MATEMÁTICAMENTE PROBADA DEL SISTEMA. EJ: RSA

SEGURIDAD PERFECTA: INICIADA POR SHANNON
EN 1949, BASADA EN LA ENTROPÍA DEL LENGUAJE Y TEORÍA DE INFORMACIÓN.

ROBUSTEZ DEPENDE TAMBIÉN DEL ESPIONAJE
O DE UN MAL DISEÑO