Implementation and Management of Systems Security
158.738

A/Prof. Julian Jang-Jaccard
Massey University

PRIVACY

What is privacy?

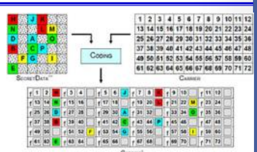
- *The state or condition of being free from public attention to the degree that you determine.*
- Before the technology, it was relatively easy to choose the level of privacy
- No longer possible. Data is automatically collected without user's knowledge or consent
- "Terms of condition" or "Privacy term" is too long or often difficult to understand

Cryptography

- Often regarded as the best tool to protect privacy
- Comes from the Greek word "Kryptos" (meaning hidden) and "Graphia" (meaning writing)
- Science of protecting information by encoding it into an unreadable format
- Store and transmit data in a form that only those intended can read and process
- Effective way of protecting sensitive information

Steganography

- It conceals the existence of the message
- Hides secret message inside a cover-image so it cannot be seen.

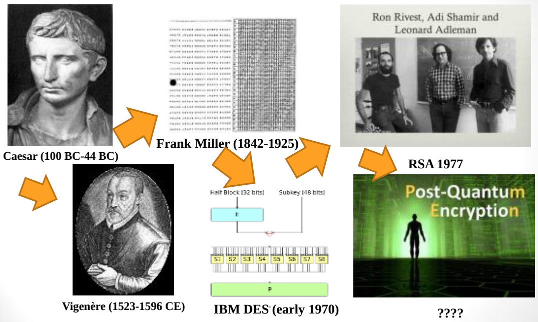


- What appears to be a harmless can contain hidden data
  - Takes the data, divides into smaller sections, and hides it in unused portion of the file

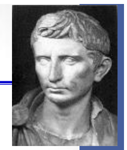
Cryptography Terms

- **Plaintext**– directly read by humans (used to be text, now its bits and bytes)
- **Ciphertext**– encrypted data
- **A cipher (or cryptographic algorithm)** – mathematics or algorithm that turns ciphertext into plaintext (and vice-a-versa)
- **Encryption**–process of "encipherment"
- **Decryption**–process of "decipherment"

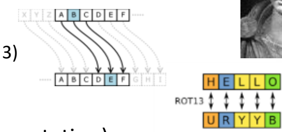
Brief History of Crypto



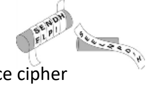
Classic Cryptography

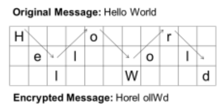


- Substitution Cipher
  - Caesar cipher (shift by 3)
  - Rot13 (shift by 13)



- Transposition (or permutation) Cipher
  - Scytale
  - Rail Fence cipher
  - Route cipher





Polyalphabetic cipher

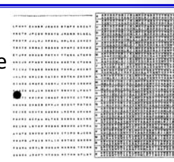
- A polyalphabetic cipher uses multiple substitution alphabets.
- Vigenere Cipher : introduces the concept of a key (that can change)

Plaintext:	ATTACKATDAWN
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR

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

One Time Pad

- Proposed by Frank Miller in 1882
- Mathematically possible to provide "the perfect secrecy" only if;
  - The key must be as long as the plain text.
  - The key must be truly random
  - The key must only be used once
  - The key must kept secret
- Nice concept but impractical!

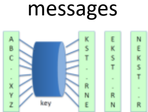


(DIANA)
The table on the right is an aid for converting between plaintext and ciphertext using the characters at left as the key.

Was heavily used in 1960s among Russians and US top secrets.

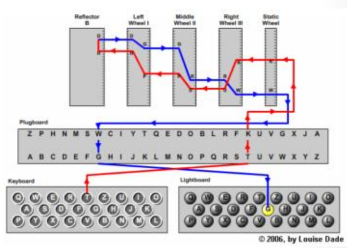
During World War I/II

- Mechanical era: a mechanical device for encrypting messages



Rotor machine

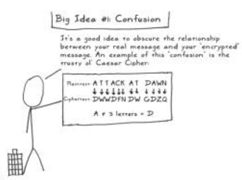
The enigma

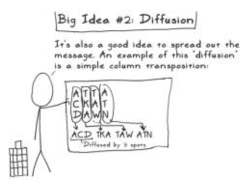


The inner workings of enigma

Two Principles

- Confusion
  - Make relationship between ciphertext and key as complex and intricate as possible
- Diffusion
  - Statistical Nature of plaintext is reduced in ciphertext



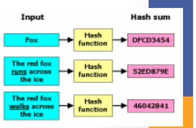


Modern Cryptography

- Modern cryptography
  - After World War I/II
  - rely on mathematics and electronic computers
- One-Way encryption
  - Hash
- Two-way encryption
  - Symmetric Algorithms
  - Asymmetric Algorithms

Hash Function

- A hash algorithm creates a unique "digital fingerprint" (= message digest or hash)
- It's a ONE-WAY function
  - Content cannot be used to reveal the original data
  - Takes a variable-length string as input
  - Returns a fixed-length string as output
- Even a small change in the input drastically changes the output
- Primarily for comparison purposes



Hash Characteristics

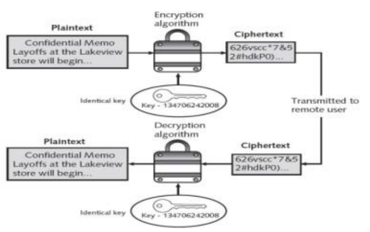
- Fixed Size.
  - Always produce the same fixed size output no matter how long the input is.
- Unique.
  - Two different sets of data cannot produce the same digest
  - Known as a collision
- Original.
  - Should not be possible to produce a desired or predefined hash
- Secure.
  - The resulting hash cannot be reserved in order to determine the original words

Hash functions

- Popular hash function MD5
  - Produce 128 bit ciphertext
  - E.g., b9b985cdc61c8db72289ce54f0937eb2 (32 hex)
  - Thoroughly broken
- Government standard SHA-1, SHA-2
  - SHA-1 : 160 bit ciphertext
  - E.g., 4751031b69d5480dfb30023f72640dd45a3c5de (40 hex)
  - Theoretical weaknesses
- "NEW" cryptographic hash function SHA-3
  - Too new to fully evaluate
  - Maybe good enough

Symmetric Algorithms

- Use the same single key to encrypt and decrypt
- The key being used must be kept private.
- Also known as a secrete key or private key algorithm

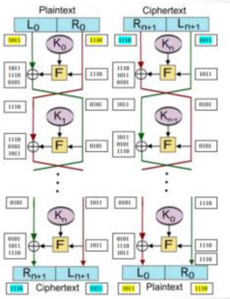


Stream vs. Block Cipher

- Stream Cipher (bit-by-bit encryption)
  - Converts one symbol of plaintext (1 bit or 1 byte)
  - Different key for each symbol
- Block cipher (block-by-block encryption)
  - Works on a given sized chunk of data at a time (fixed size)
  - Different key for a different block
  - Most of current ciphers use Block cipher

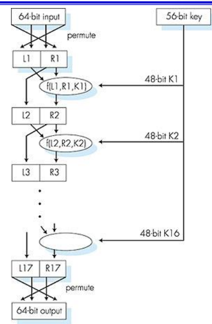
Feistel Architecture

- The father of block cipher encryption model
- Consisting multiple rounds of processing (depends on desired security)
- Each round consisting of a "substitution" step followed by a permutation step
- Encryption and decryption procedures almost identical



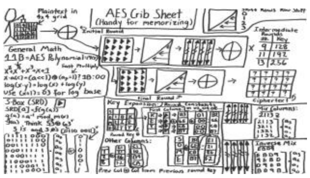
DES

- Data Encryption Standard (1977)
- Developed by IBM (Lucifer) improved by NSA
- Based on Feistel Cipher
- Works on 64 bit block with 56 bit keys
- Brute force attack – broken within a day or two
- Extension: 3DES



AES

- Advanced Encryption Standard (2001)
  - Joan Daemen & Vincent Rijmen
  - Block size 128 bits
  - Key can be 128, 192 or 256 bits



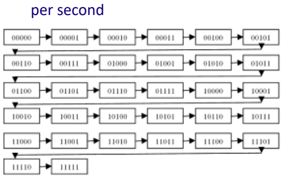
Source: the original concept drawing of AES

Symmetric Encryption

- Key must be distributed
  - Vulnerable to interception (an important weakness)
  - Key management – a challenge
  - Tend to be efficient
- Strength of encryption
  - Length of the secret key - longer keys more difficult to crack (more combinations to try)
  - Not necessary to keep the algorithm secret
- How to break an encryption
  - Brute force: try all possible combinations until the correct key is found
  - Cryptanalytics

Short Keys

- Besides frequency analysis and other methods, can try to brute force it! (Brute force = try all combinations)
- How long should a key be? It depends upon the power of the attacker.
- GPUs can test 100s of millions of symmetric cryptographic systems per second



(a) Brute forcing K size = 5

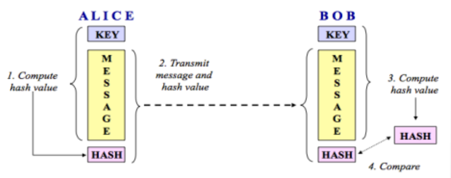
Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Brute Force Attacks

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years

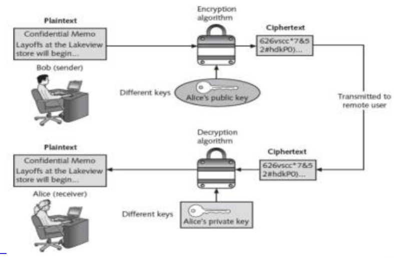
Message Authentication Code

- message came from the state sender and has not changed during the transit
- Provides both message authentication and message integrity



Asymmetric Algorithms I

- Use two keys to encrypt and decrypt instead of only one
- Also known as public key algorithm



Asymmetric Algorithms II

- Key pairs.
  - Unlike symmetric algorithm that uses only one key, it requires a pair of keys
- Public key.
  - By their nature are designed to be "public". Do not need to be protected.
  - Can be freely given o anyone or posted on the Internet
- Private key.
  - Must be kept confidential and never shared
- Both directions.
  - Keys can work both directions

Encryption Vs. Hash

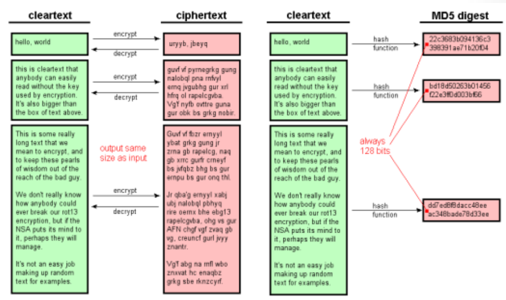


Fig. 1: Encryption - a two-way operation

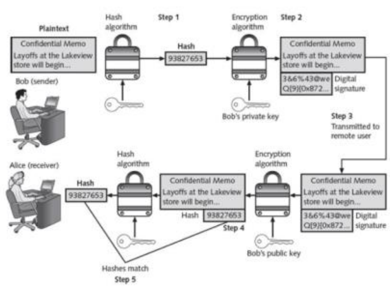
Fig. 2: Hashing - a one-way operation

Source: http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Digital Signatures

- A handwritten signature on a paper document serves as proof that the signer has read and agreed to the document
- A digital signature works same but more;
  - Verify the sender: confirm the identity of the person where the electronic message originated
  - Prevent the sender from denying (or disowning) the message: cannot claim the signature was forged.
  - Prove the integrity of the message: Message not altered since it was signed

Digital Signature



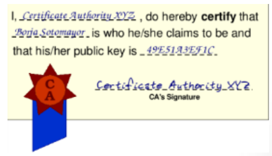
Key comparison

Security Goal	Hash	MAC	Digital Signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-repudiation	No	No	Yes
Key	None	Symmetric keys	Asymmetric keys

Non-repudiation: cannot deny the authenticity of the sender of the document.

Digital Certificate

- Problem: How to trust that a public key belong to whom it claims to be?
- Solution: Use trusted third-party entity.
  - They vouch that a public key belongs to a particular individual or organization
- Most common:
  - X.509 certificate



Public Key Infrastructure (PKI)

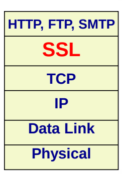
- Set of hardware, software, organizations, and policies to make Public Key Cryptography work on Internet
  - How to verify that the person sending the message
- Certificate Authority (CA)
  - A trusted organization that can vouch for the authenticity of the person or organization
- Certificate
  - A digital document verifying the identity of a digital signature's source
  - Contains the public key of an entity, signed by the CA
  - In other words, a certificate allows CA to vouch for an entity's identity in a verifiable manner.

Public Key Infrastructure (PKI)

- User registers with a CA (e.g. VeriSign) and requests for an X.509 certificate
  - a Certificate Signing Request (CSR) is sent to CA
  - Must provide some proof of Identity
  - Levels of certification: simple email confirmation or background checks
- CA issues the digital certificate (signed by CA)
- User attaches the certificate to transactions (email, web, etc)
- Receiver authenticates transaction with CA's public key
  - Contact CA to ensure the certificate is not revoked or expired

Secure Sockets Layer (SSL)

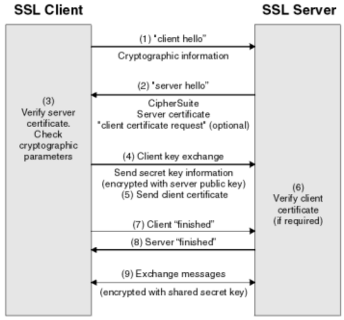
- A protocol widely used on the Web
  - Between the application and transport layers
- Operations of SSL
  - Encrypts outbound packets from transport layer
  - Negotiation for cryptographic parameters:
    - hash algorithm
    - signing algorithm
    - encryption algorithm
  - Communications encrypted by using the keys negotiated



Transport Layer Security (TLS)

- Same thing as SSL
  - From SSL3.0, it is now called TLS for legal reason and marking purpose
- Protocol most widely used on the Web
- Can be used with various applications
  - For example, if used with HTTP => HTTPS
  - If used with SMTP => SMTPS

SSL/TSL Handshake Protocol



END