CA169: Week 7

Computer Security

TYPES OF SECURITY

- Network security
- Network traffic security
- Physical Security
- Application Security

NETWORK SECURITY

- Stop hackers from getting into network
- Penetration testing (pen testing) to determine weak points in network
- Cryptography service for passwords
- Firewalls
- White/Blacklisting

SECURING NETWORK TRAFFIC

- Provide encryption for all traffic
- HTTP v HTTPS
- Prevent hackers from getting access
  - Man in the middle attach
- Prevent network disruption
  - DOS or DDOS

SECURITY ISSUES

- Confidentiality
  - Only authorised people should have access to information.
  - The General Data Protection Regulation (GDPR) covers data protection for individuals.
- Authentication
  - Provide correct identification of the source of a message which is verifiable and reliable
- Integrity
  - Only authorised people with correct access privileges should have access to viewing, altering, delaying or filtering data held or transmitted in an information environment
- Nonrepudiation
  - Neither the sender or the receiver of information may be able to deny that a transmission took place. Useful for financial transactions.
- Access Control
  -
- Availability
  - Information and media should be available to authorised people when needed
- Legal Issues
  - Many countries in Europe do not even allow the transmission of encrypted data, it may be a criminal offence to be involved in such activities, so check before sending encrypted email and such.
  - The US does not allow the export of cryptographic software or hardware, they regard such systems to be armaments, with severe penalties for infringements.

HACKERS

- Black Hat
  - Entirely for financial gain
  - Malicious
- Grey Hat
  - Good or bad
- White Hat
  - Ethical Hacker
  - E.g. Works as security penetration tester

YOU CAN PROTECT YOURSELF

- Know your enemy
  - Open Web Application Security Project™ https://www.owasp.org
- Defend yourself
  - Set traps: (E.g. honeypots https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html)
- Develop your expertise:
  - Facebook capture the flag
  - DEFCON: https://www.defcon.org/
  - Hack this site: https://www.hackthissite.org/

ATTACKS

- Hacking requires in depth knowledge of the target setup
- Windows or Linux?
- What language (php, python, javascript)
- What web framework ? (Node, Django, Rails, Wordpress…)

CRYPTOLOGY

- Cryptography – writing or solving codes
  - Devise encryption and decryption methods
- Cryptanalysis – analysing codes and breaking them
  - Find out patterns in the code

CRYPTANALYSIS - PROBLEMS

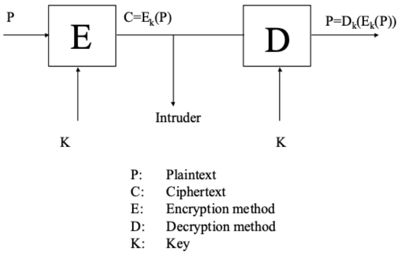
- Ciphertext only
  - Only have encrypted data and nothing else
  - Hardest kind of problem to solve
- Known plaintext problem
  - Some matching plaintext and ciphertext
- Chosen plaintext
  - Arbitrary amounts of plaintext and ciphertext available

A CRYPTOGRAPHIC SYSTEM

1. Plaintext P is passed to an encryption module
2. P is then encrypted using encryption key K making the ciphertext C
3. (optional) an intruder intercepts C but it is encrypted
4. C is then decrypted with a decryption key K to produce the plaintext P

CIPHERS

- One of the oldest methods of encryption
- Push letters up (or down) a number of spaces on the alphabet
- Oldest cipher (Caesar cipher) replaces text by 3 places (A becomes D, B -> E etc..)
- Key K = 3
- Zhofrph wr frpsxwhu qhwzrunv wz.

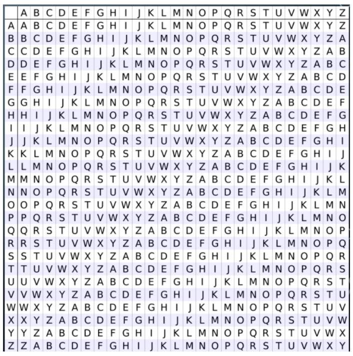


CIPHERS - SUBSTITUTION CIPHERS

- One of the oldest methods of encryption
- Push letters up (or down) a number of spaces on the alphabet
- Oldest cipher (Caesar cipher) replaces text by 3 places (A becomes D, B -> E etc..)
- Key K = 3
- Welcome to computer networks two.
- Replacing one letter with another is called monoalphabetic substitution
- There are 26 letters, the means that there are 26! Possibilities (4 × 1026)
- Generating all possible answers is called brute force cracking
- The time taken to brute force the cipher “khoor zruog” (hello world) is 31,000 years ! (2019-2020 computing power)
- However, language exhibits statistical properties that can be exploited
- Frequency analysis examines common letters and pairs to crack the password

CIPHERS – POLYALPHABETIC CYPHERS

- Use multiple Caesar ciphers
- Vigenère cipher
- Use repeating phrase as key (phrase repeatsmuntil its length matches the plaintext)
- E.g “Hello world” with key “howareyouh”
- Becomes: “oshlf amffk”



	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

CIPHERS - TRANSPOSITION CIPHERS

- Reorder the letters but otherwise do not change them
- E.g. encrypt “Hello World”

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

4	5	1	2	3
H	E	L	L	O
W	O	R	L	D

- LRLLODHWEO

CIPHERS – PRODUCT CIPHERS

- Mix and match multiple substitution and transposition ciphers back to back
- Work off the binary representation of ASCII
- The Data Encryption Standard (DES) uses a product cipher system
- DES can be broken due to its small key size 56 bits
-

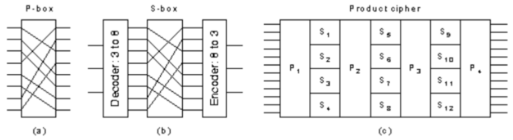


Fig. 7-4. Basic elements of product ciphers. (a) P-box. (b) S-box. (c) Product.

From: *Computer Networks*, 3rd ed. by Andrew S. Tanenbaum, ©1996 Prentice Hall

DES – DATA ENCRYPTION STANDARD

- Adopted by US Gov. in 1977
- No longer secure in original form, modified form still useful however
- Uses 19 stages product cipher, 56 bit key
- Uses S-box and P-box mixing

IDEA – INTERNATIONAL DATA ENCRYPTION ALGORITHM

- Lai and Massey in 1990,1992
- 128 bit key, immune to brute force attacks
- What else has 128 bits?
- Input is the same as DES, 64 bit blocks of plaintext

IDEA - STRENGTHS

- 64 bit blocks, enough to stop statistical analysis
- 128 bit key length stops brute force attacks (for now)
- Can be further strengthened using cipher feedback
- Confusion introduced by adding dependencies between the plaintext and ciphertext
- Three different mathematical operations (DES only uses 1)
    - Bitwise XOR
    - MOD 2^{16} addition
    - MOD 2^{16} + 1 multiplication
- Diffusion each plaintext bit has influence over each ciphertext bit. Plaintext is spread over a large amount of ciphertext, so statistical structure of the plaintext is hidden

PUBLIC KEY CRYPTOGRAPHY

- The key used must be kept secret
- In PKC the decryption key is kept secret, but the encryption key is public
- Practically impossible to guess the decryption key from the encryption key

PKC – STRONG ENCRYPTION

- Based on trap door functions, easy to solve in one direction but extremely difficult to reverse
- Multiply two prime numbers p and q which is easy to solve
- But working backwards is incredibly difficult

RSA ALGORITHM

- Pre-compute the parameters
- Divide plaintext into blocks (bit-strings) P s.t. 0<=P<n
- To encrypt
    - $C = P^{e}$ MOD $_{n}$
- To decrypt
    - $P = C^{d}$ MOD $_{n}$