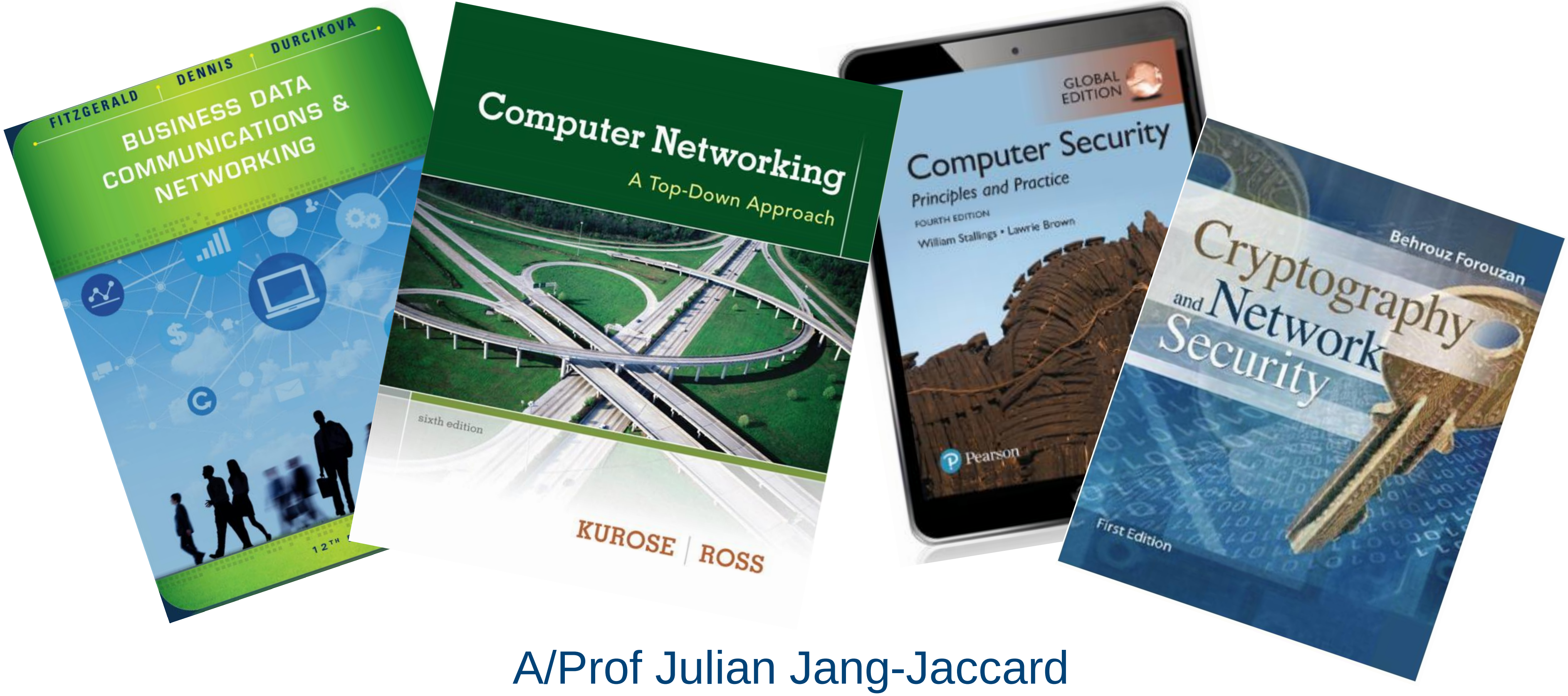
MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Network, Security and Privacy

158.235



A/Prof Julian Jang-Jaccard

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Introduction to Privacy (Cryptography)

What is Privacy?

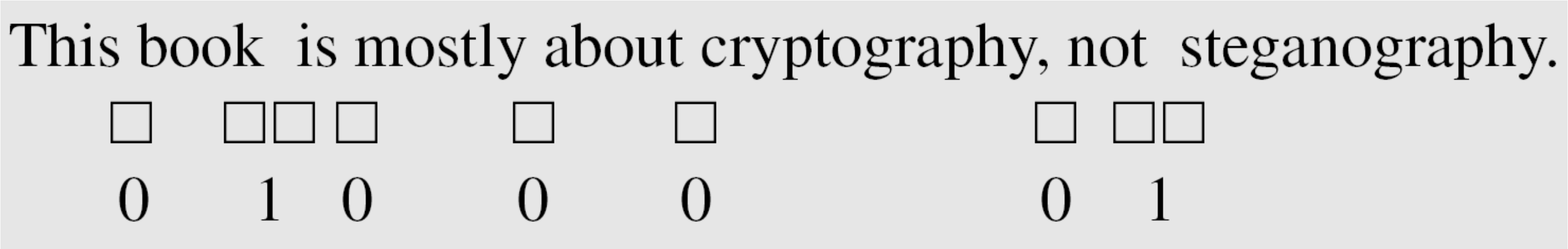
- *The state or condition of being free from public attention to the degree that you determine.*
- Before the technology, it was relatively easy to choose the level of privacy
- No longer possible. Data is automatically collected without user's knowledge or consent.
- "Terms of condition" or "Privacy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

Cryptography

- Often regarded as the best tool to protect privacy (via providing mechanisms to meet Confidentiality, Integrity, Authentication etc.,)
- Comes from the Greek word “Kryptos” (meaning secret) 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.
- The word steganography, with origin in Greek, means “covered writing,” in contrast with cryptography, which means “secret writing.”
- Hides secret message inside a cover-image so it cannot be seen.
- Example: covering data with text



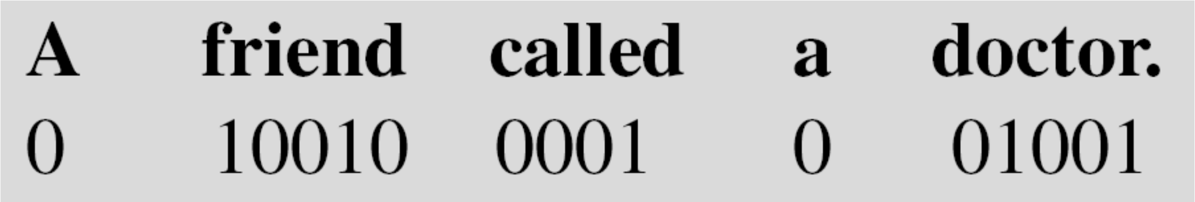
This book is mostly about cryptography, not steganography.

□ □□ □ □ □ □ □□

0 1 0 0 0 0 1

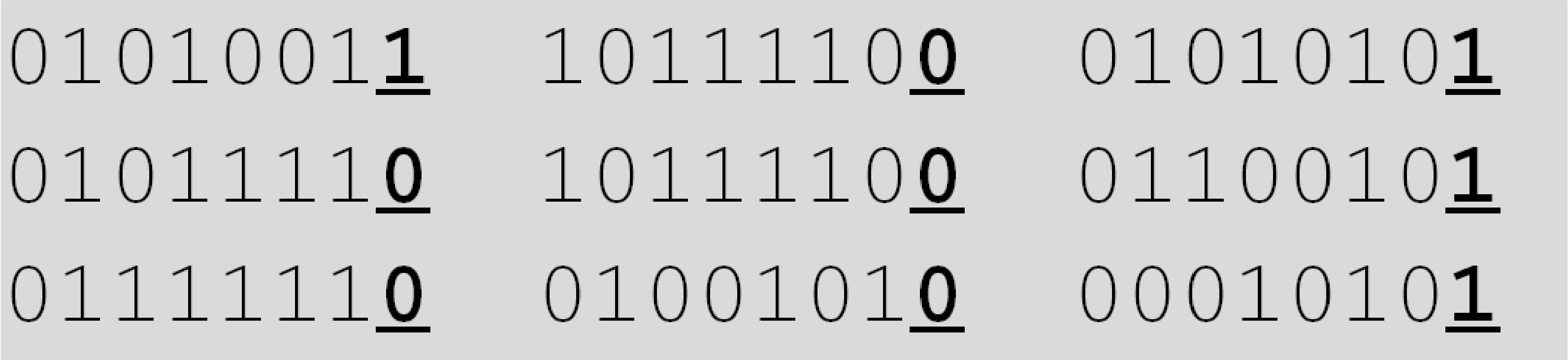
Steganography?

- Example: using dictionary



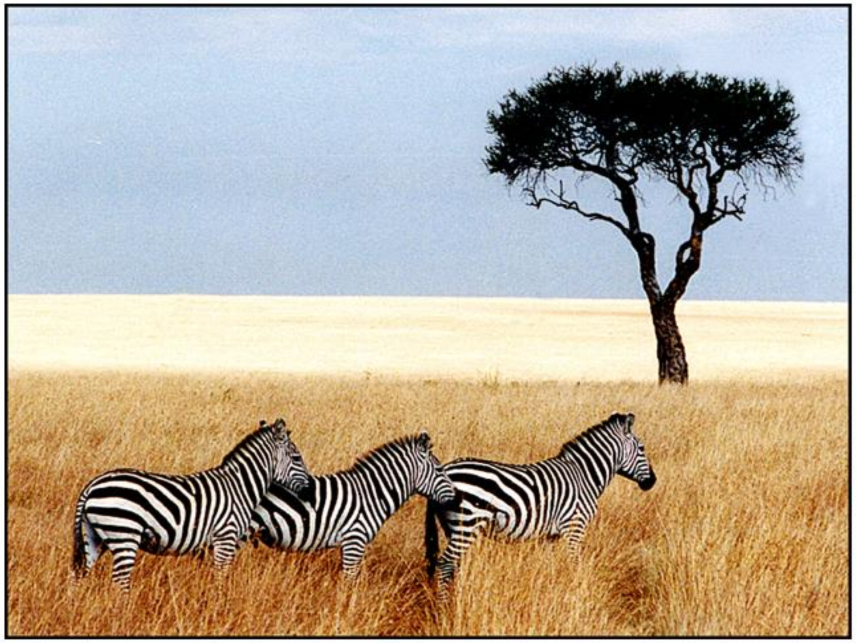
A	friend	called	a	doctor.
0	10010	0001	0	01001

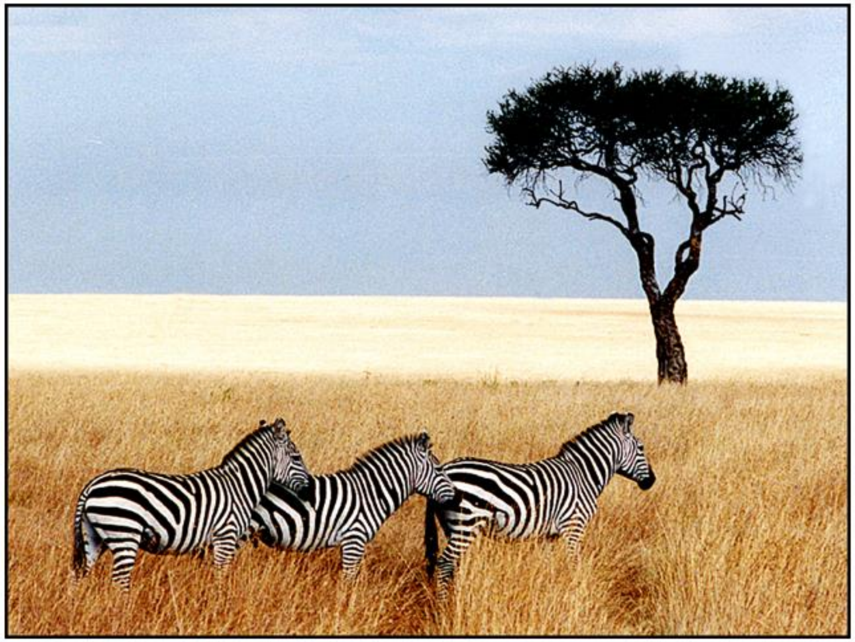
- Example: covering data under color image



0101001**1**	1011110**0**	0101010**1**
0101111**0**	1011110**0**	0110010**1**
0111111**0**	0100101**0**	0001010**1**

Which one is applied of a Steganography?

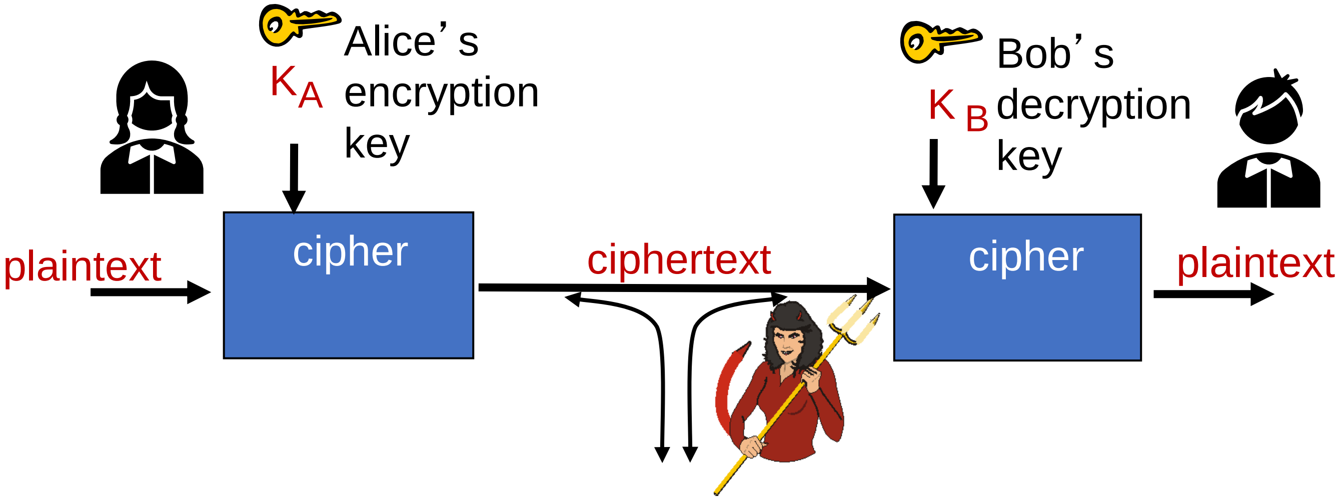




Cryptography Terms

- 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 creating a ciphertext from a plaintext (using a cipher)
- Decryption–process of creating a plaintext from a ciphertext (using a cipher)

Cryptography Terms

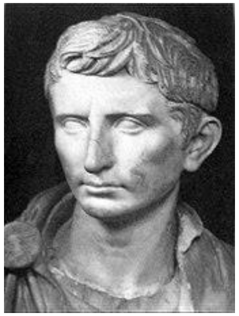


m plaintext message

$K_A(m)$ ciphertext, encrypted with key K_A

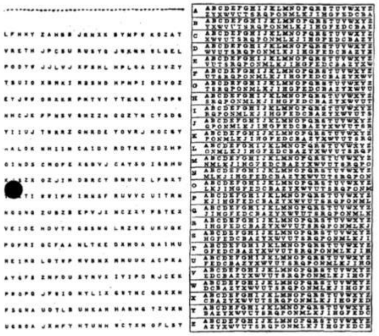
$m = K_B(K_A(m))$

Brief History of Cryptography

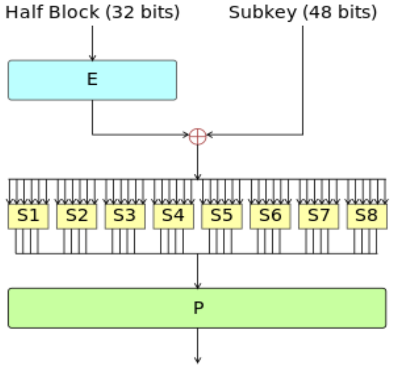


Caesar (100 BC-44 BC)

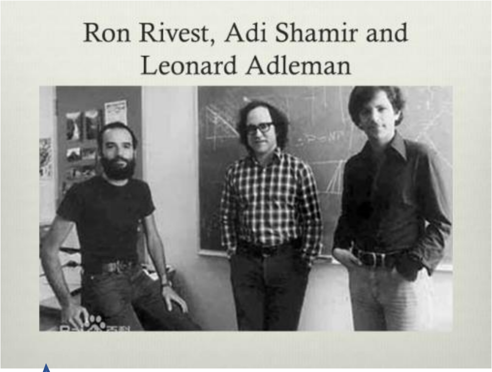
Vigenère (1523-1596 CE)



Frank Miller (1842-1925)

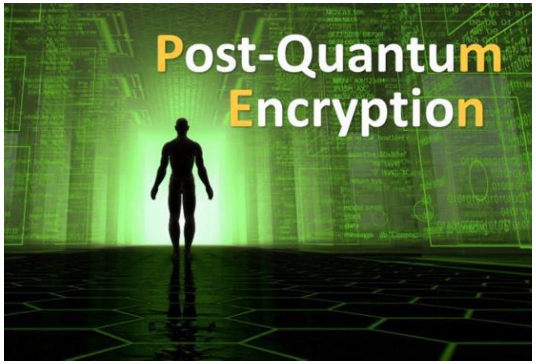


IBM DES (early 1970)



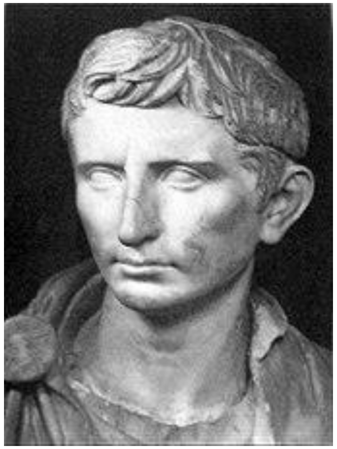
Ron Rivest, Adi Shamir and Leonard Adleman

RSA 1977

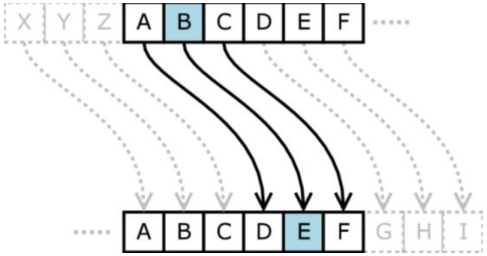


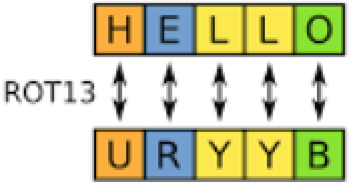
Ongoing

Classic Cryptography

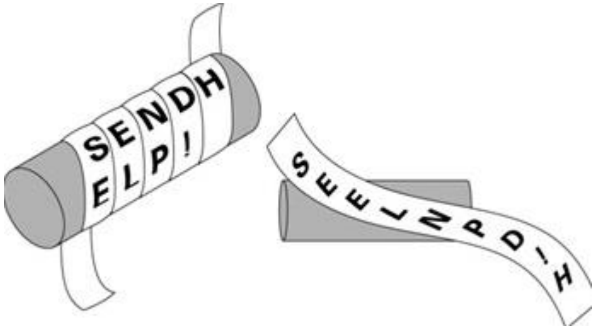


- Substitution Cipher
  - Caesar cipher (shift by 3)
  - Rot13 (shift by 13)

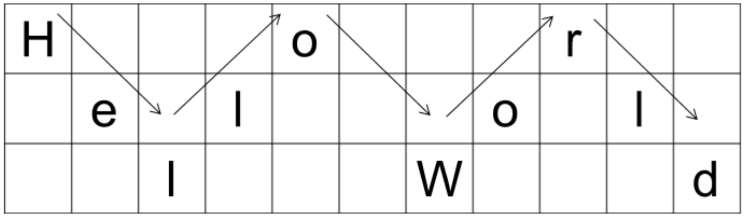




- Transposition (or permutation) Cipher
  - Scytale
  - Rail Fence cipher
  - Route cipher



Original Message: Hello World



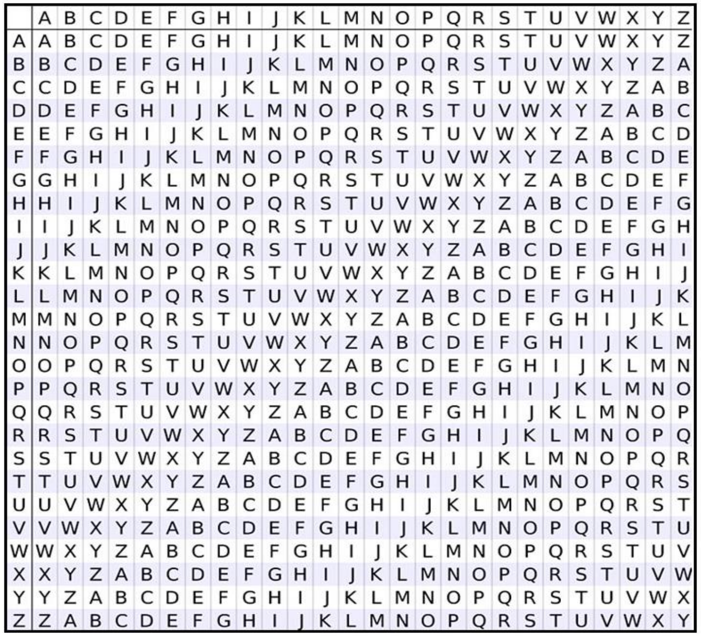
H				o				r		
	e		l				o		l	
		l				W				d

Encrypted Message: Horel ollWd

Polyalphabetic Cipher

- A **polyalphabetic cipher** is any cipher based on substitution, using multiple substitution alphabets.
- Vigenere Cipher: introduces the concept of a key (that can change)

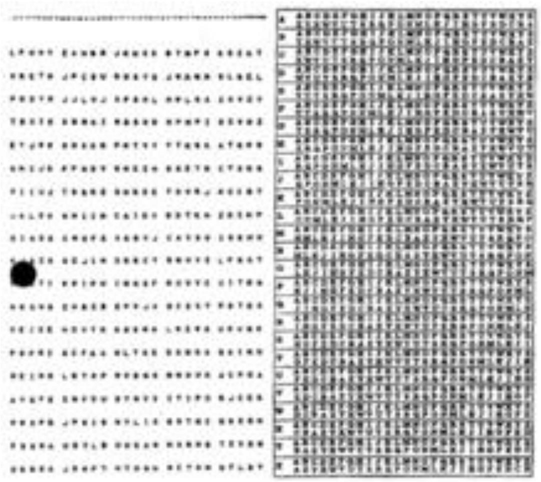
Plaintext:	ATTACKATDAWN
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR



	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 keep secret
- Nice concept but impractical!



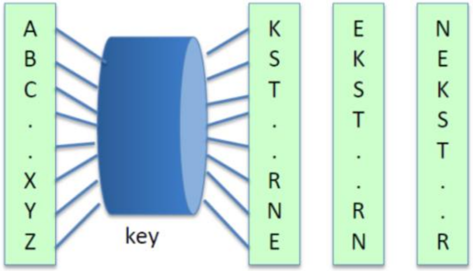
(DIANA - Codebook)

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

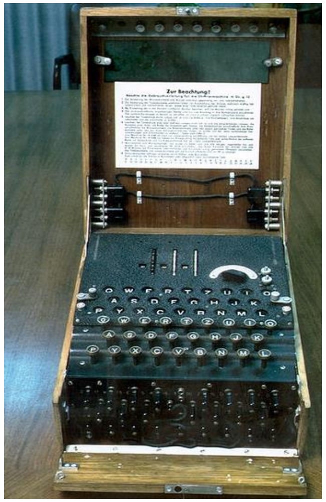
Was heavily used in 1960s among Russians and US top secrets.

During World War I/II

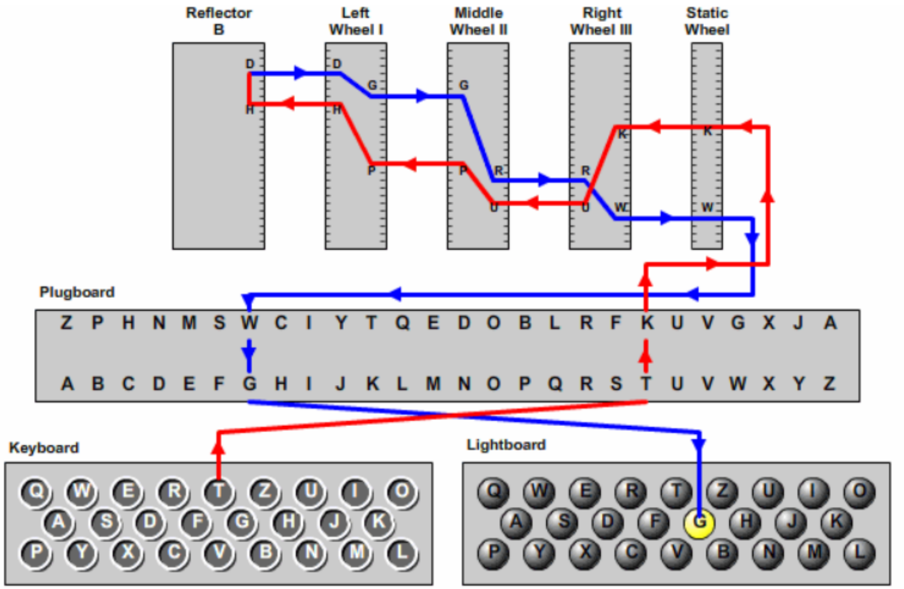
- Mechanical era: a mechanical device for encrypting messages



(a) Rotor machine



(b) enigma machine


Reflector B
Left Wheel I
Middle Wheel II
Right Wheel III
Static Wheel
Plugboard
Z P H N M S W C I Y T Q E D O B L R F K U V G X J 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
Keyboard
Lightboard

© 2006, by Louise Dade

(c) The inner workings of enigma

Two Principles

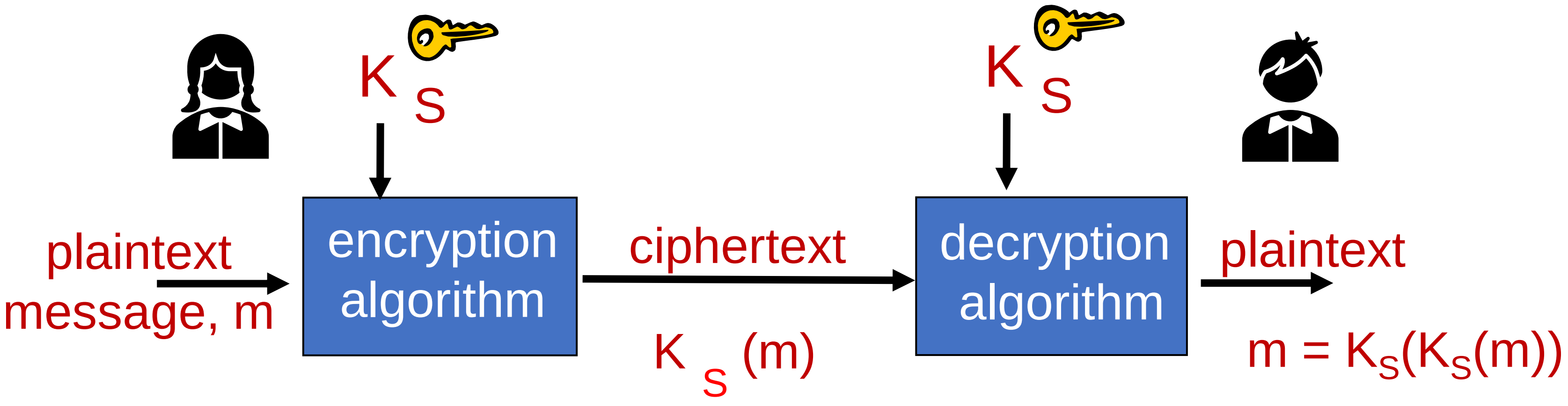
- Confusion
  - Making the relationship between ciphertext and key as complex and intricate as possible
  - To hide the relationship between the ciphertext and the key
  - Makes it difficult to find the key from the ciphertext
  - If a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected
  - Provided by (advanced) substitution techniques
- Diffusion
  - The redundancy in the statistical nature of plaintext is reduced in the statistics of the ciphertext
  - To hide the relationship between the ciphertext and the plaintext
  - Provided by transposition techniques

Modern Cryptography

- Symmetric Cryptography
  - Use the same key to both encrypt and decrypt a message

- Public-Key Cryptography
  - Use two separate keys (but same algorithm), one for encryption and the other for decryption

Symmetric Cryptography



symmetric key crypto: Bob and Alice share same (symmetric) key: K

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

Q: how do Bob and Alice agree on key value?

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

```
 plaintext:  abcdefghijklmnopqrstuvwxyz

ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

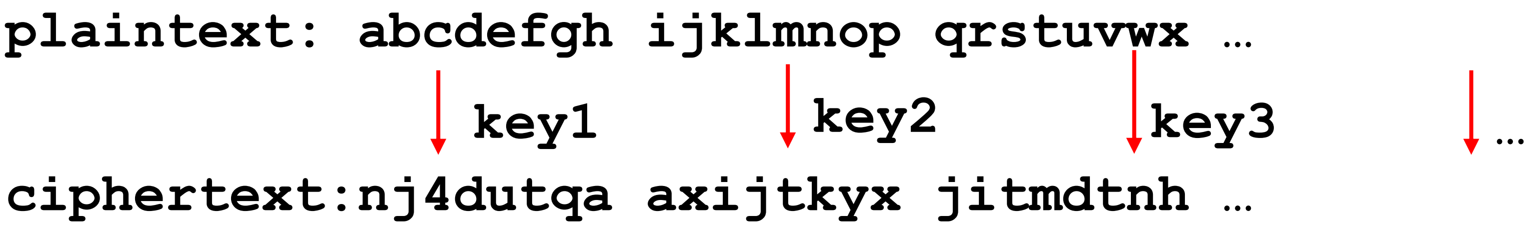
e.g.:

```
 Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Encryption key: mapping from set of 26 letters
to set of 26 letters

Stream vs. Block Cipher

- 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

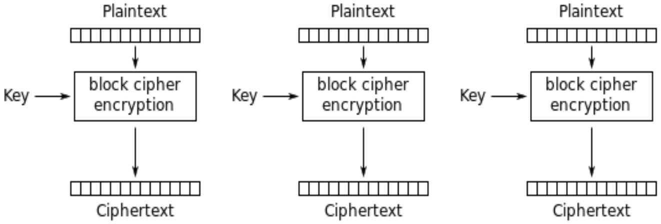


```
plaintext: abcdefgh ijklmnop qrstuvwx …
                   key1      key2      key3        …
ciphertext:nj4dutqa axijtkyx jitmdtnh …
```

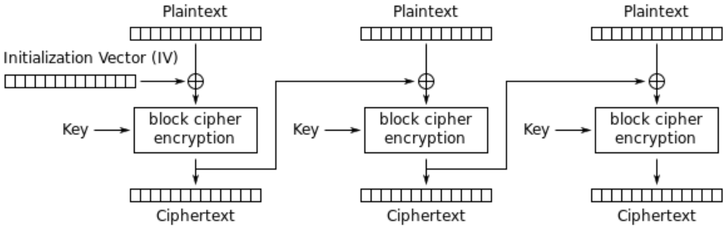
Encryption key: key1, key2, key3, …

Block Cipher Modes

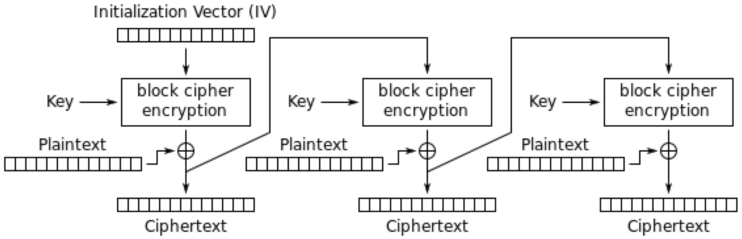
- These are procedural rules for a generic block cipher
- Different modes result in different results (ciphertext) achieved.
- Cover a wide variety of applications
- NIST defines 5 modes
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback Mode (CFB)
  - Output Feedback Mode (OFM)
  - Counter Mode (CTR)



Electronic Codebook (ECB) mode encryption



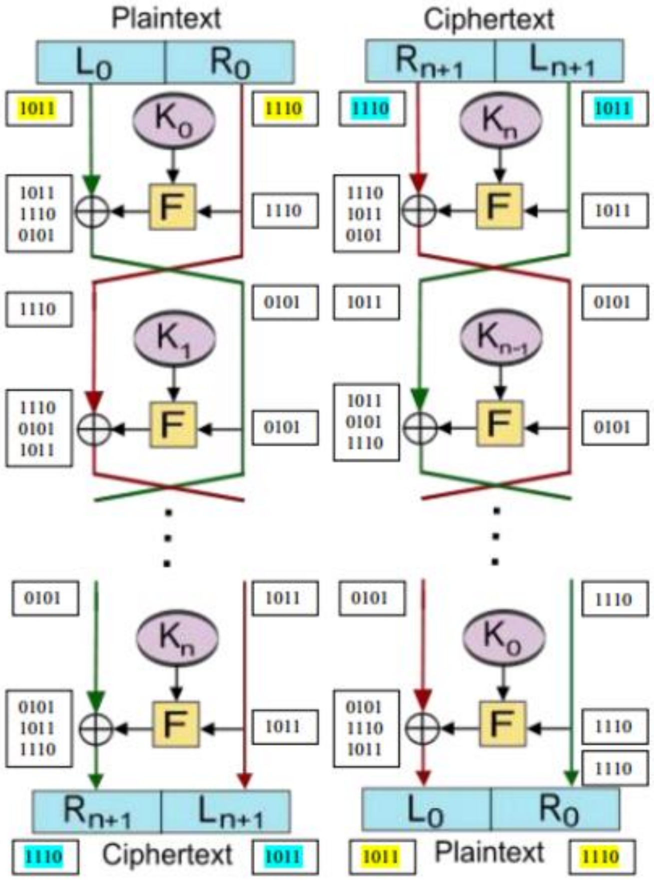
Cipher Block Chaining (CBC) mode encryption



Cipher Feedback (CFB) mode encryption

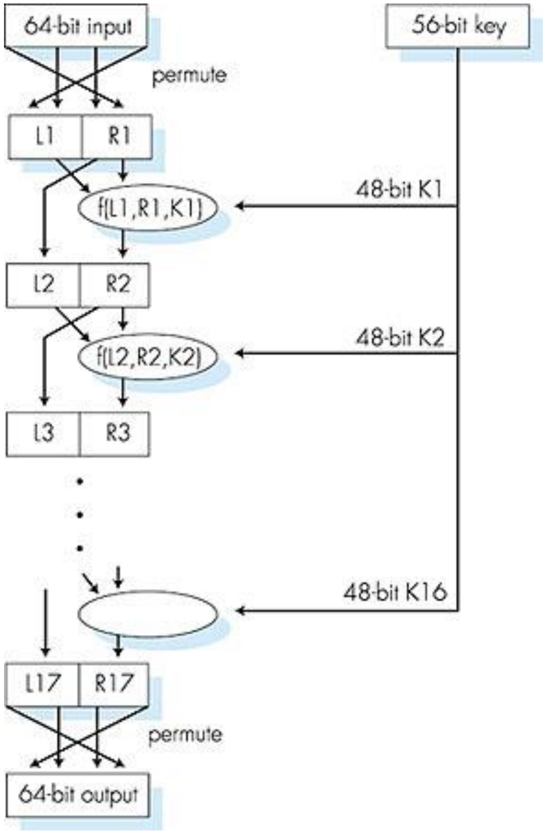
Fiestel Architecture

- 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



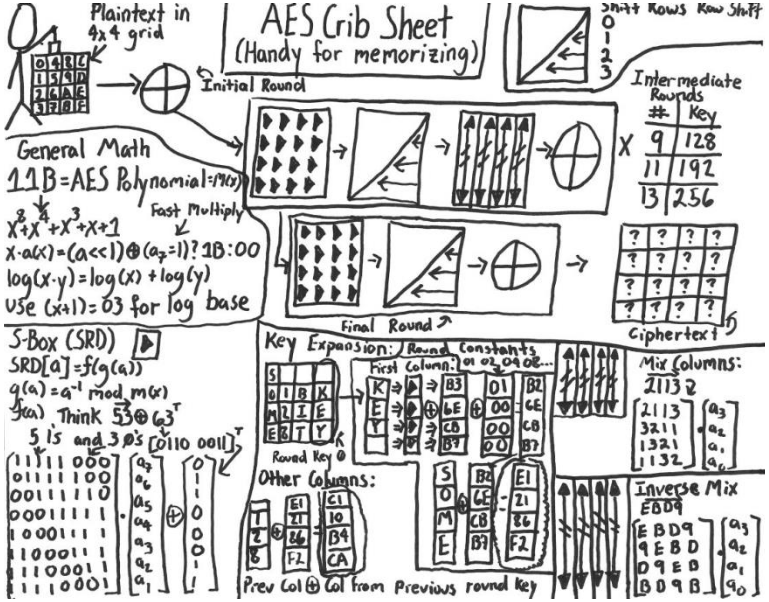
DES

- 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 – still broken



AES

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

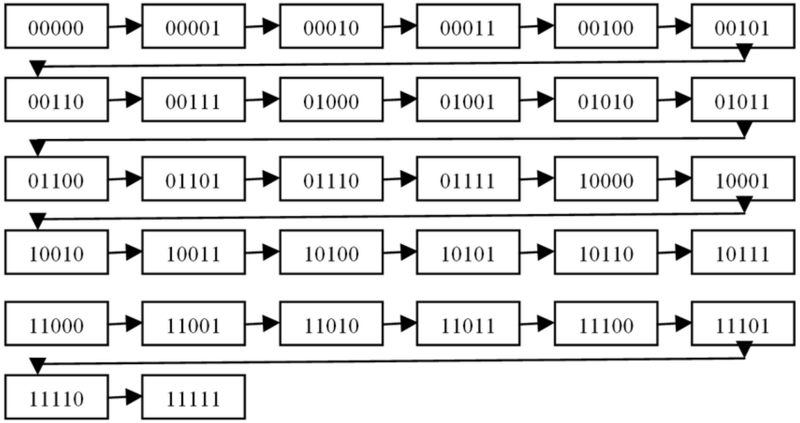


Symmetric Cryptography

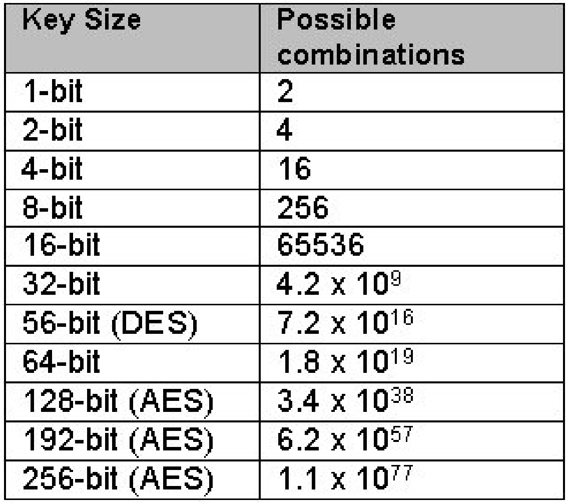
- Key must be distributed
  - Vulnerable to interception (an important weakness)
  - Key management – a challenge
  - Tend to be inefficient
- Strength of encryption
  - Length of the secret key - longer keys more difficult to crack (more combinations to try)
  - Not necessary to keep the algorithm secret

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

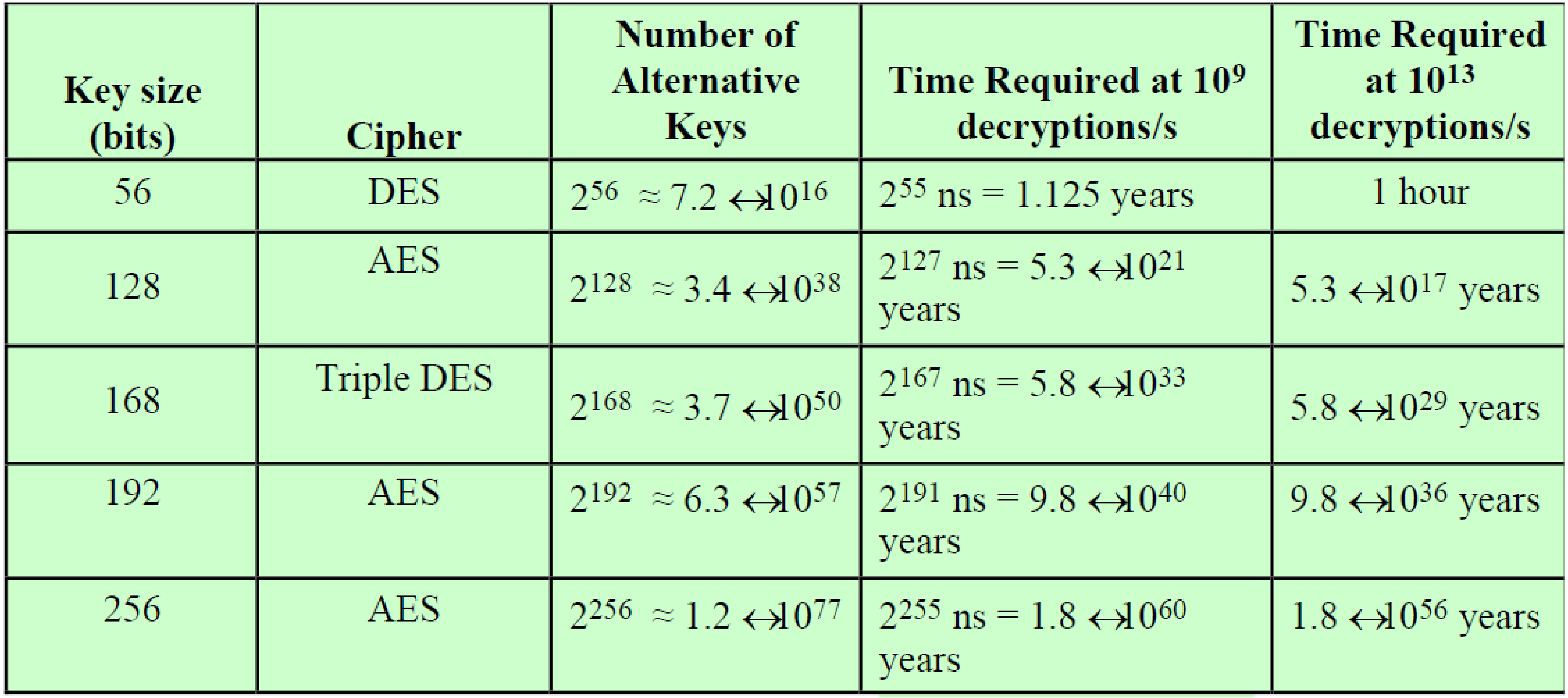


(a) Brute forcing K size = 5



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

Brute Force Attacks

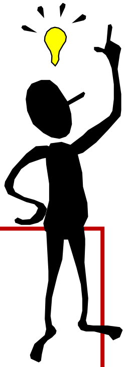


Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \leftrightarrow 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \leftrightarrow 10^{38}$	2^{127} ns = $5.3 \leftrightarrow 10^{21}$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

Symmetric Encryption

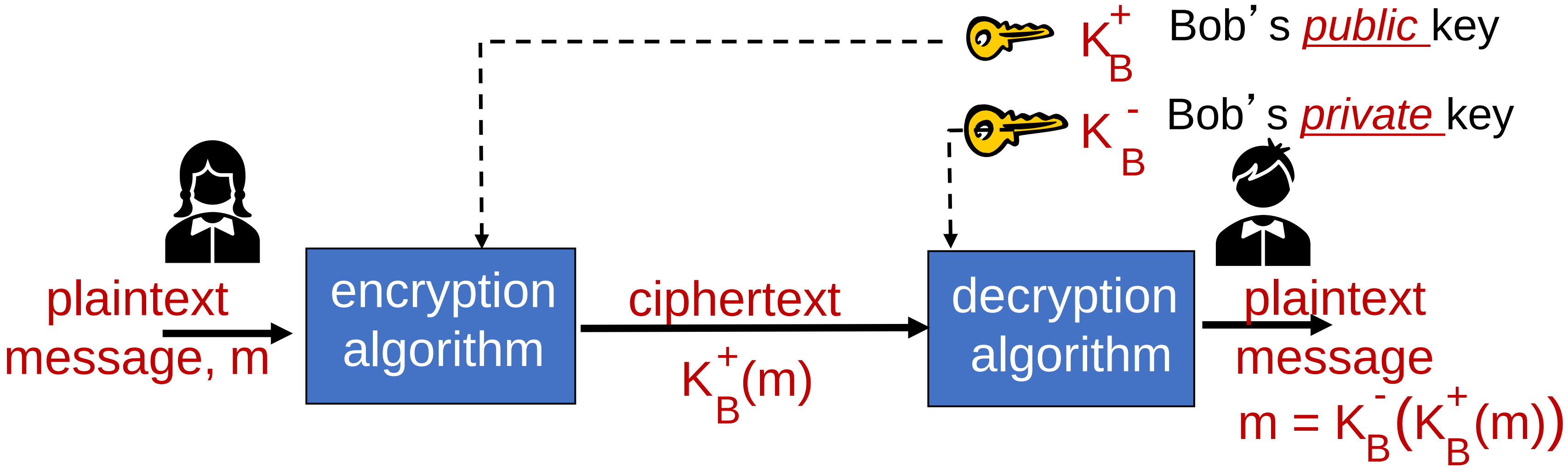
- symmetric key crypto
  - requires sender, receiver know shared secret key
  - Q: how to agree on key in first place (particularly if never "met")?

public key crypto



- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver do *not* share secret key
- *public* encryption key known to *all*
- *private* decryption key known only to receiver

Public key cryptography



K_B^+ Bob’s *public* key

K_B^- Bob’s *private* key

plaintext message, m

encryption algorithm

ciphertext

$K_B^+(m)$

decryption algorithm

plaintext message

$m = K_B^-(K_B^+(m))$

1. need $K_B^+(\ )$ and $K_B^-(\ )$ such that $K_B^-(K_B^+(m)) = m$

2. given public key K_B^+, it should be impossible to compute private key K_B^-

Public key cryptography

- 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 to anyone or posted on the Internet
- Private key.
  - Must be kept confidential and never shared
- Both directions.
  - Keys can work both directions

RSA: Creating public/private key pair

1. choose two large prime numbers p, q. (e.g., 1024 bits each)
2. compute $n = pq$, $z = (p-1)(q-1)$
3. choose e (with $e<n$) that has no common factors with z (e, z are "relatively prime").
4. choose d such that $ed-1$ is exactly divisible by z. (in other words: $ed \bmod z = 1$).
5. *public* key is $\underbrace{(n,e)}_{K_B^+}$. *private* key is $\underbrace{(n,d)}_{K_B^-}$.

RSA: encryption, decryption

0. given (n,e) and (n,d) as computed previously,

1. to encrypt message m ($<n$), compute

   $c = m^{e} \bmod n$

2. to decrypt received bit pattern, c, compute

   $m = c^{d} \bmod n$

magic happens! $m = (\underbrace{m^{e} \bmod n}_{c})^{d} \bmod n$

RSA example:

Bob chooses *p=5*, *q=7*. Then *n=35*, *z=24*.

e=5 (so *e*, *z* relatively prime).
d=29 (so *ed-1* exactly divisible by z).

encrypting 8-bit messages.

encrypt: $\underbrace{m}_{12}$ $\underbrace{m^e}_{248832}$ $\underbrace{c = m^e \bmod n}_{17}$

decrypt: $\underbrace{c}_{17}$ $\underbrace{c^d}_{481968572106750915091411825223071697}$ $\underbrace{m = c^d \bmod n}_{12}$

RSA

$$\underbrace{K_B^-(K_B^+(m))}_{\substack{\text{use public key first,}\\ \text{followed by}\\ \text{private key}}} = m = \underbrace{K_B^+(K_B^-(m))}_{\substack{\text{use private key}\\ \text{first, followed by}\\ \text{public key}}}$$

result is the same!

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

END