MONASH University
Information Technology

FIT2093 INTRODUCTION TO CYBER SECURITY

Week 2 Lecture

Cryptography I:

Symmetric Key Encryption

Part 1

Principles for CONFIDENTIALITY


Outline

Symmetric Cryptography

Part 1: Basic Concepts

- CONFidentiality problem
- Cryptography: big picture
- Encryption: Classical Ciphers
- Encryption: Modern Cipher **principles**

Part 2: Modern Encryption Algorithms

- Block ciphers
  - Design requirements
  - Case study I: Data Encryption Standard (DES)
  - Case study II: Advanced Encryption Standard (AES)
- Block Cipher Modes: How to use block ciphers for encryption
  - ECB, CBC, CTR

MONASH University

CONFidentiality Problem

The CONF Problem: Insecure Channel vs Secrecy

- Aim: vs Insecure channel / storage

- **Strategy**
  - *accept* fact: channel insecure
    - whatever sent, could be intercepted (eavesdropping)

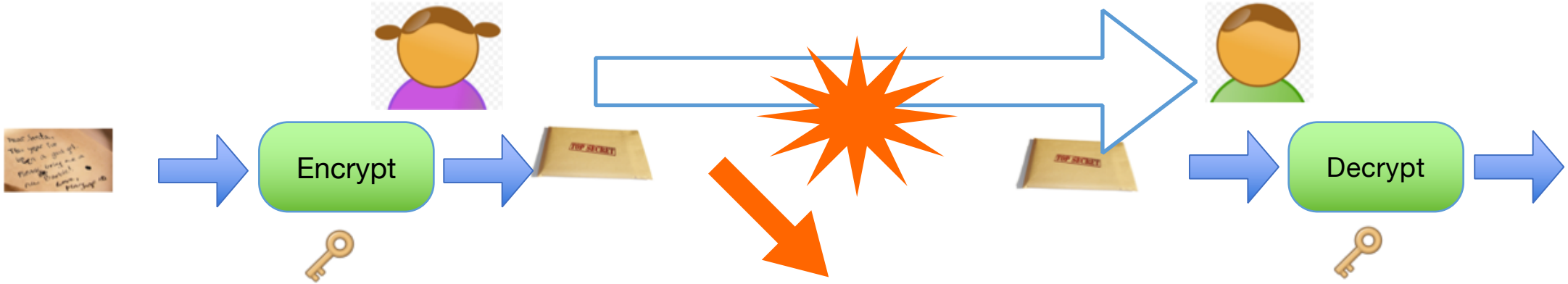
    - no control over channel

CONFidentiality : How?

- Aim: reveal nothing: secrecy / confidentiality **(CONF)**

- **Strategy**
  - ***accept*** fact: whatever sent, could be intercepted (eavesdropping)
  - prevent
    - even if intercepted, not reveal secret info
    - scramble info before send, s.t. only Rx can descramble

      (encrypt) (decrypt)
    - use secret (key) s.t. only Rx can decrypt



Note: free images from freeimages.com

CONFidentiality: How?

Symmetric Crypto

- Goal: secret data remains CONFidential

- Means:
  - not all can access
  - only some can access

- Q: how to enforce?
  - access control: check who, & grant access
  - encryption:
    - lock, only some have key
    - scramble / mix up, only some can undo

Security Principle(s)

- State **what can't** be solved/avoided, aim for **next best**

  e.g. channel insecure, cannot avoid interceptions

  so next best: **don't** let intercepted things **reveal** info

  - *change* means: "prevent interception" "wrap it up"

    (physically secure the channel) (secure the sent info)

- be fluid: the **means** could be varied , as long as same **goal** achieved eventually
  - x prevent interception, that's ok
  - so prevent revelation of info


CONFidentiality: How?

Symmetric Crypto

- Goal: secret data remains CONFidential

- Means:
  - not all can access, only some can access

- How?
  - encryption: cannot access anymore
  - decryption: to access again, undo the encryption
    - only some can decrypt (*restricted reversal*)
    - how?
      - keep algorithms secret
      - use extra (secret) input (the key)

CONFidentiality: via Obscurity?

Symmetric Crypto

- … only **some** can decrypt …
- How?
  - keep algorithms secret

CONFidentiality: Kerckhoffs' Principle

Symmetric Crypto


- … only **some** can decrypt …
- How?
  - use extra (secret) **input** (called the **key**)

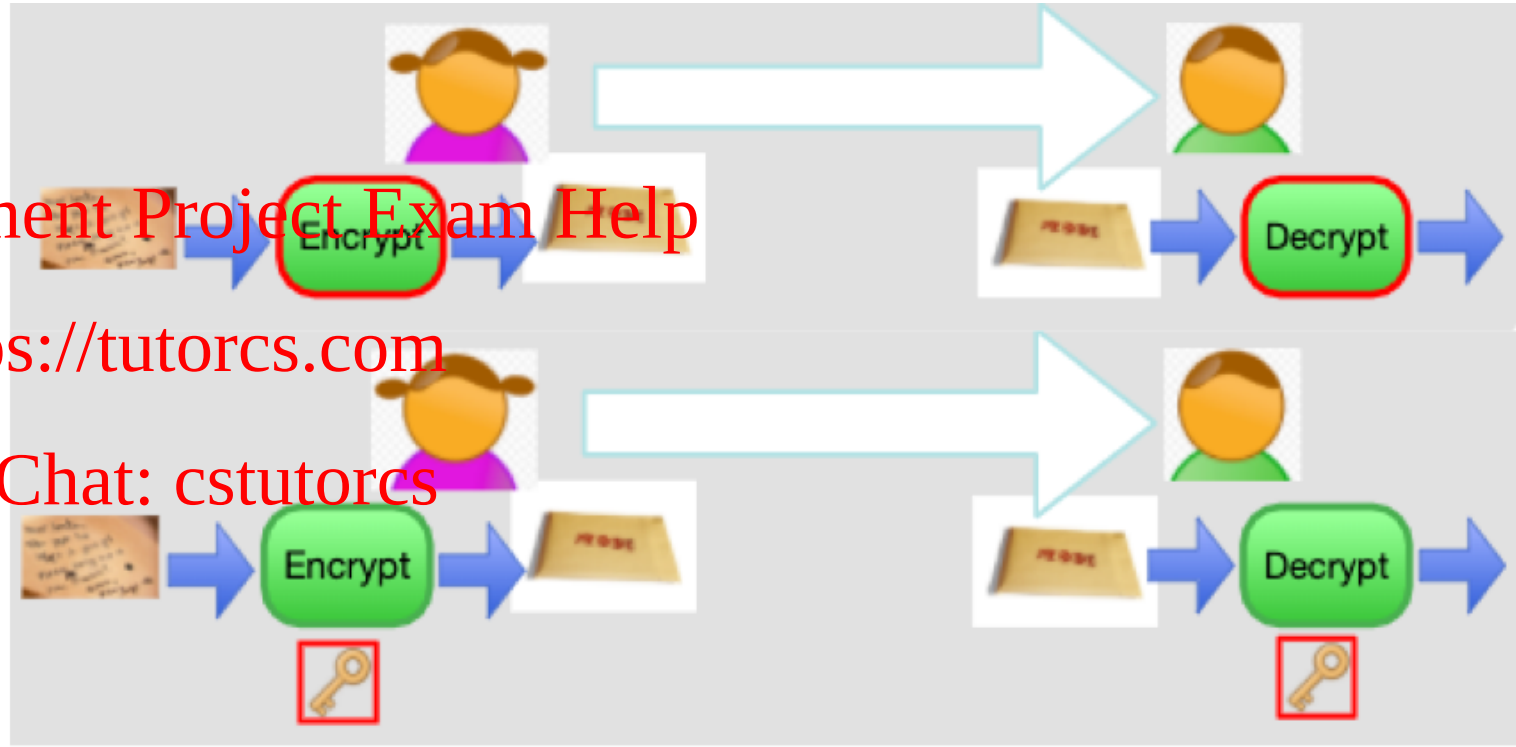
CONFidentiality

Symmetric Crypto

- keep algorithms secret: security by obscurity

- keep key secret: security by Kerckhoffs' principle

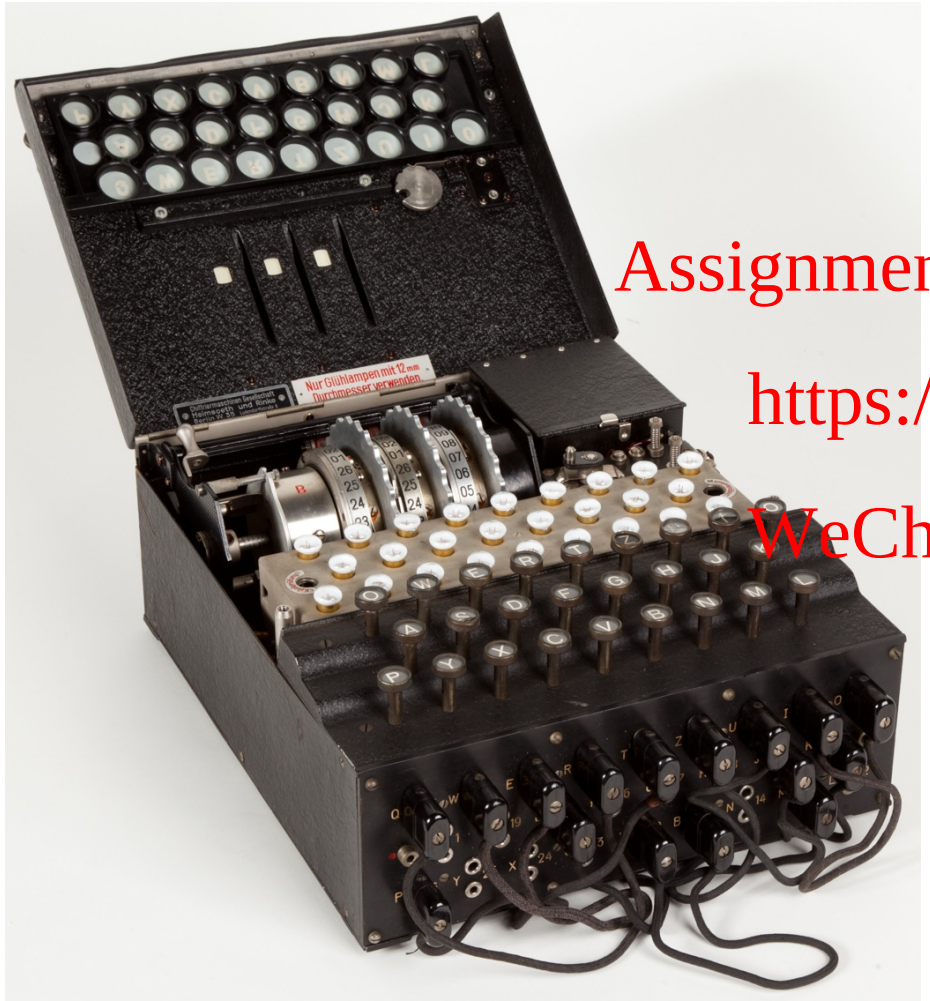
- Q: which one do you think is harder to do: Keeping an **algorithm** secret or a **key** secret? Why?

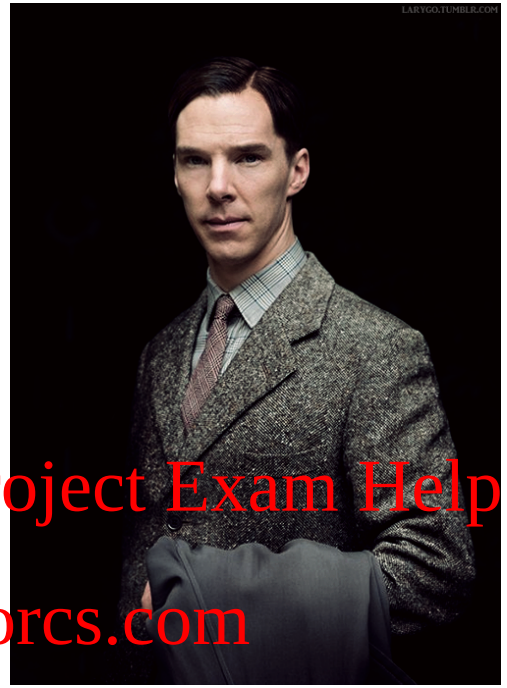


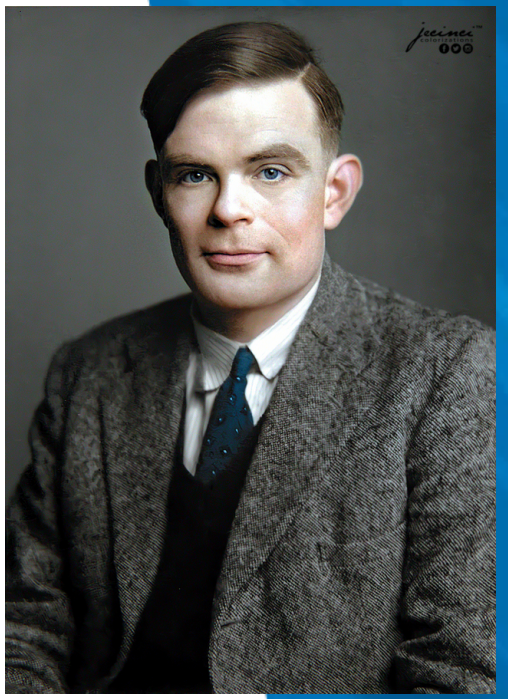
Activity (5 mins)

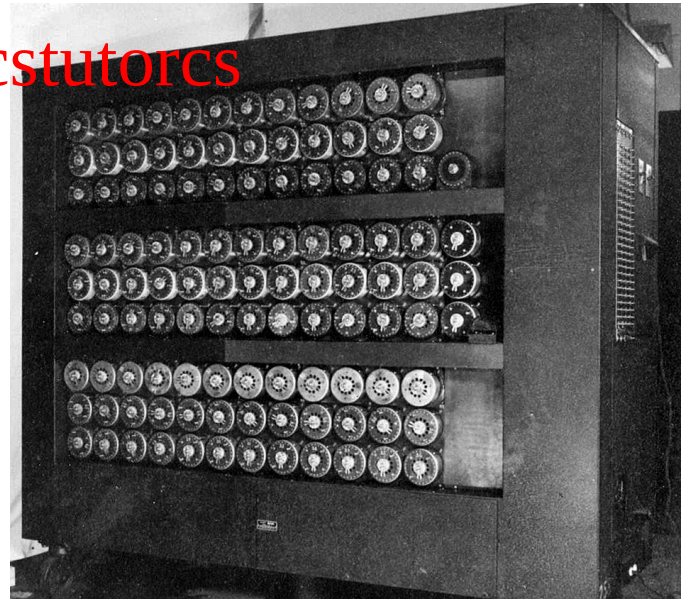
1) Click the latest link in the Zoom chat
2) Add your question response to the Ed forum

A hint from history…









MONASH University

Cryptography: Big Picture

Cryptography: Big Picture

Symmetric Crypto

- CONFidentiality: achieved via Encryption (weeks 2-4)
  - Two types of encryption:
    - Symmetric key (week 5)
    - Public Key (weeks 6-7)

- INTegrity achieved via (week 5)
  - Message Authentication Code (MAC) – symmetric key
  - Digital Signatures – public key

- AUTHentication achieved via (week 5)
  - Digital Signatures – public key

Cryptography: Big Picture

Symmetric Crypto

Cryptography - Terminology

- plaintext p ⟶ Encryption ⟶ ciphertext c
- message m ⟶ MAC ⟶ tag τ
- message m ⟶ DigitalSignature ⟶ signature s

  ...
- Cryptography:
  - techniques that **transform** the input (message) such that output allows to achieve CONF, INT, AUTH, ...

  - History
    - from Greek words kryptos (hidden) & graphein (writing)
    - initially: study of message **secrecy** (hidden writing) aka CONF, now covers many other security goals

Cryptography vs Cryptanalysis

Symmetric Crypto

Cryptography - Terminology

- Cryptography: by cryptographer
  - how to design to achieve security
- Cryptanalysis: by cryptanalyst
  - how to break / analyse security
  - offers security assurance to others about your design

MONASH University

Encryption: Classical Ciphers

Cryptography: Classical

Symmetric Crypto

- Mostly about encryption
  - e.g. Caesar Cipher [during Julius Caesar's time]
  - Enigma [by Germany during World War II]
- Classical Ciphers: two types of basic operations
  - Substitution
  - Transposition

Cryptography: Classical

Symmetric Crypto

- Substitution
  Systematically **substitute** (group of) letters with other (group of) letters … like **table lookup**
- *Example*: change each letter with another letter that is two positions down in the English alphabet sequence: “message” => “oguucig”

- Transposition
  Rearrange the **position** of the letters in the message according to some rules: **not depend on value** of letter(s)
- *Example*: Move each letter in the message by 1 position: “message” => “emessag”

Classical Example: Caesar Cipher

Symmetric Crypto

- Caesar cipher:
  - a **substitution** cipher, named after Julius Caesar

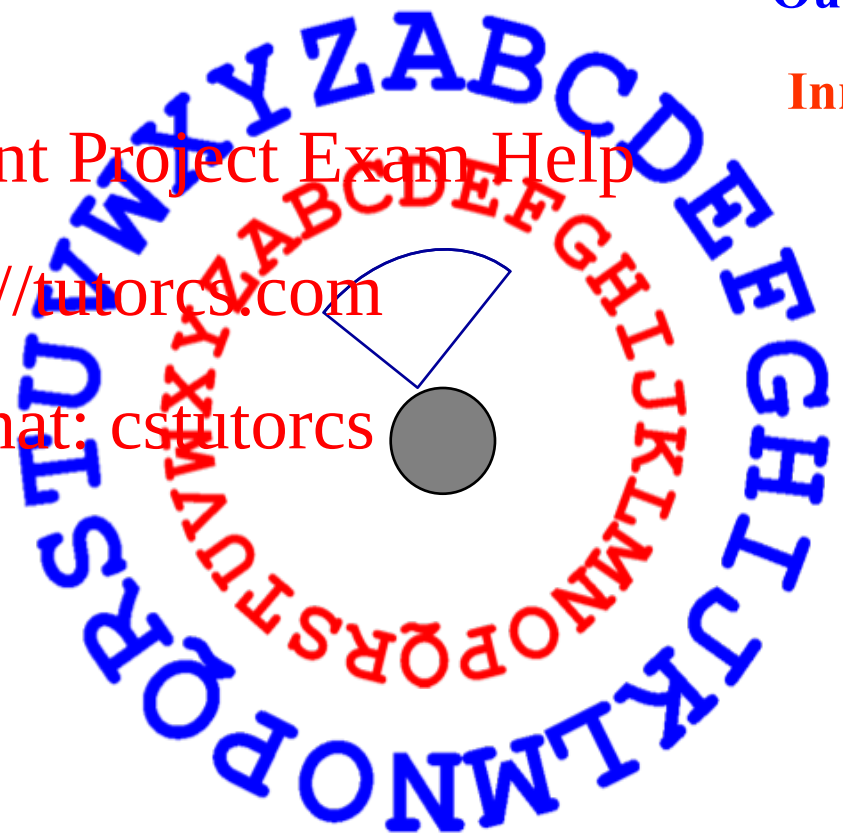
- How it works:
  each letter is substituted with the letter *a fixed number of positions* after it in the alphabet table

- The **number of positions** is the key both for encryption and decryption: should not let others know how many number of positions

Classical Example: Caesar Cipher

Symmetric Crypto

- K=3 ... Shifted by three characters



Classical Example: Caesar Cipher

Symmetric Crypto

- Caesar Cipher can be viewed as modulo operation
- **Encryption:**
  - Let *x* be the position of plaintext letter to be replaced, *n* be number of positions to be shifted to find the replacement (ciphertext) letter

    i.e the key is the value of *n*
  - $E_n(x) = (x+n) \bmod 26$ & substitute that character in that position
- **Decryption:**
  - $D_n(x) = (x-n) \bmod 26$

Classical Example: Caesar Cipher

Symmetric Crypto

- for a key K = 3,
  - plaintext letter: ABCDEF...PQRSTUVWXYZ
  - ciphertext letter: DEFGHI...STUVWXYZABC

e.g. **TREATY IMPOSSIBLE**

is translated into

WUHDWB LPSRVVLEOH

- Play with the online Caesar cipher here: https://cryptii.com/pipes/caesar-cipher

Caesar Cipher: Attack

Symmetric Crypto

- Q: How to attack the Caesar Cipher?
- A: by brute force exhaustive search for the key
  - Q: what is the key?
- Attack time complexity is very low
  - can be easily broken
  - Q: how many possible keys?
  - Q: how to check a guess for key?
  - Q: how long would it take?

Activity (5 mins)

1) Click the latest link in the Zoom chat
2) Add your question response to the Ed forum

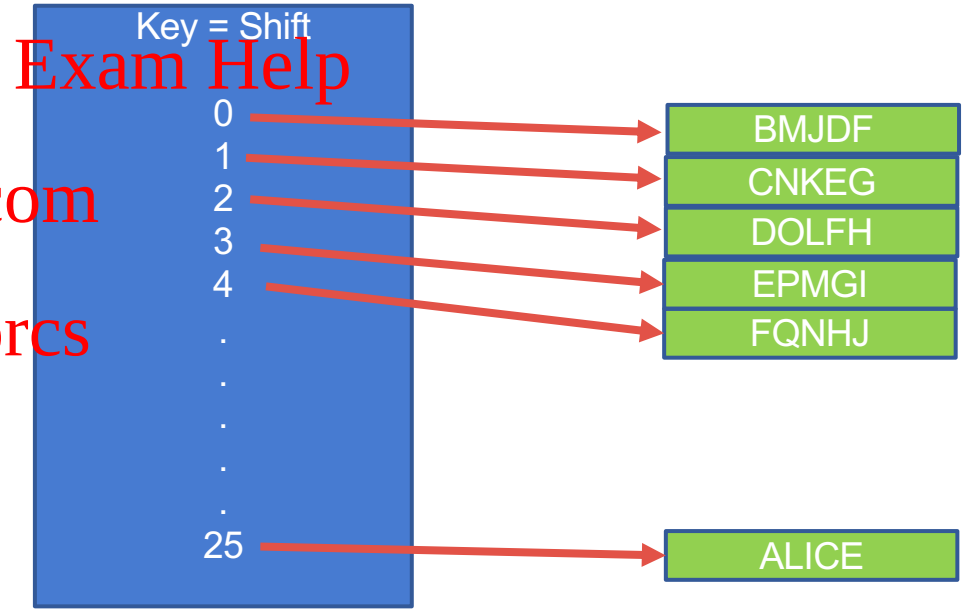
Caesar Cipher: Attack example

BRUTE FORCE ATTACK ON CAESAR CIPHER

LET'S SAY WE ARE USING CAESAR TO ENCRYPT THE NAME "ALICE", THERE WILL BE ONLY 26 POSSIBILITIES:

ONLY ONE OF THE 26 POSSIBLE DECRYPTIONS WILL TYPICALLY MAKE SENSE

E.G. BRUTE FORCE ATTACK ON CIPHERTEXT = "BMJDF"



Caesar Cipher: Attack

Symmetric Crypto

- Security of the Caesar Cipher
  - insecure against brute force exhaustive key search
- Attack complexity
  - how many guesses?
    - how many possible shifts = 26 (too small!)
  - effort to check each guess
    - see if it's English

Example II: Monoalphabetic Substitution Cipher

Symmetric Crypto

- Build a (mapping) table that **maps** a character with the replacement character

  Q: How is this cipher different from Caesar cipher?

- Need this table (in fact column 2) to encode/decode messages
  - *assuming the alphabets in column 1 is in a known sequence, else column 1 also needed*

- Different people can use different tables

A	D
B	A
C	I
D	B
E	J
F	C
G	H
H	K
…	…
Z	F

Example II: Monoalphabetic Substitution Cipher

Symmetric Crypto

- Build a (mapping) table that **maps** a character with the replacement character
- Q: What property(ies) does this table need to satisfy?
- Q: How many such mapping tables are possible for 26 upper-case English alphabets?
  - 26! Mapping tables. Why?

A	D
B	A
C	I
D	B
E	J
F	C
G	H
H	K
…	…
Z	F

Monoalphabetic Substitution Cipher: Security

Symmetric Crypto

- Alphabet substitution (mapping) table
  - can be thought of as a key:
  - Number of possible keys N = 26! ~ 4 x 10^{26}
  - Brute force key search is infeasible (millions of years)

Q: Assume each key guess takes 1 ns = 10^{-9} sec to check.

How long would brute force key search take?

Activity (5 mins)

Add your question response to the Ed forum

A	D
B	A
C	I
D	B
E	J
F	C
G	H
H	K
…	…
Z	F

Monoalphabetic Substitution Cipher: Security

Symmetric Crypto

- But, is Monoalphabetic cipher secure against **other cryptanalysis attacks**?
  - No, an efficient statistical frequency analysis attack:
    - Observation:
      - each plaintext letter always encrypts to same ciphertext letter
      - so:
      - letter repeat in plaintext letter

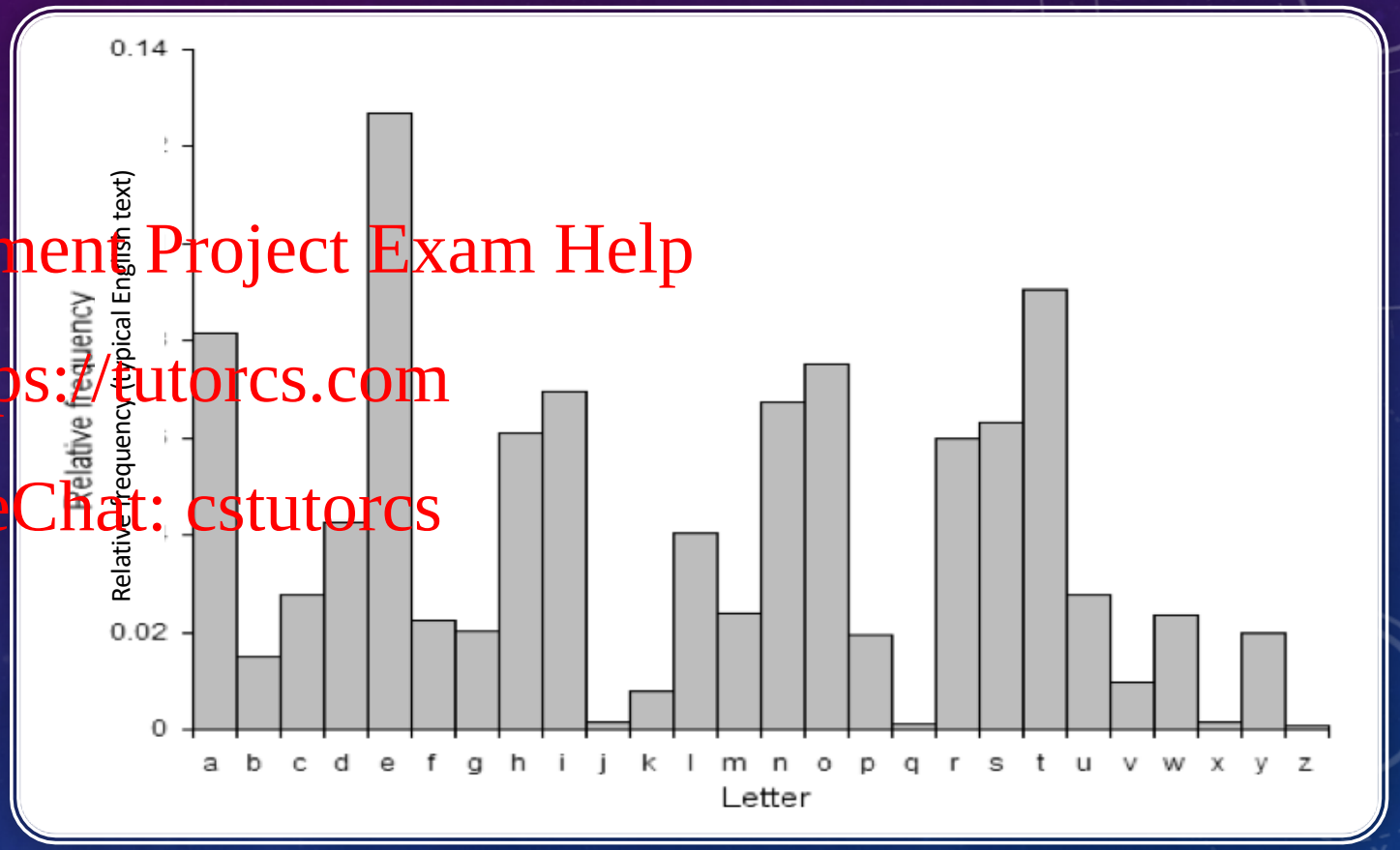
        → repeat in ciphertext !
      - cipher weakness: ciphertext letter frequencies are equal to corresponding plaintext letter frequencies
    - Fact: letter frequency in English gives lots of info on letter
      - use fact with above weakness to break the cipher!

A	D
B	A
C	I
D	B
E	J
F	C
G	H
H	K
…	…
Z	F

CRACKING THE MONOALPHABETIC SUBSTITUTION CIPHER: FREQUENCY ANALYSIS ATTACK

- By using frequency analysis with following **assumptions**:
  - Messages are in English form
  - The message is long enough to see the repetitive patterns

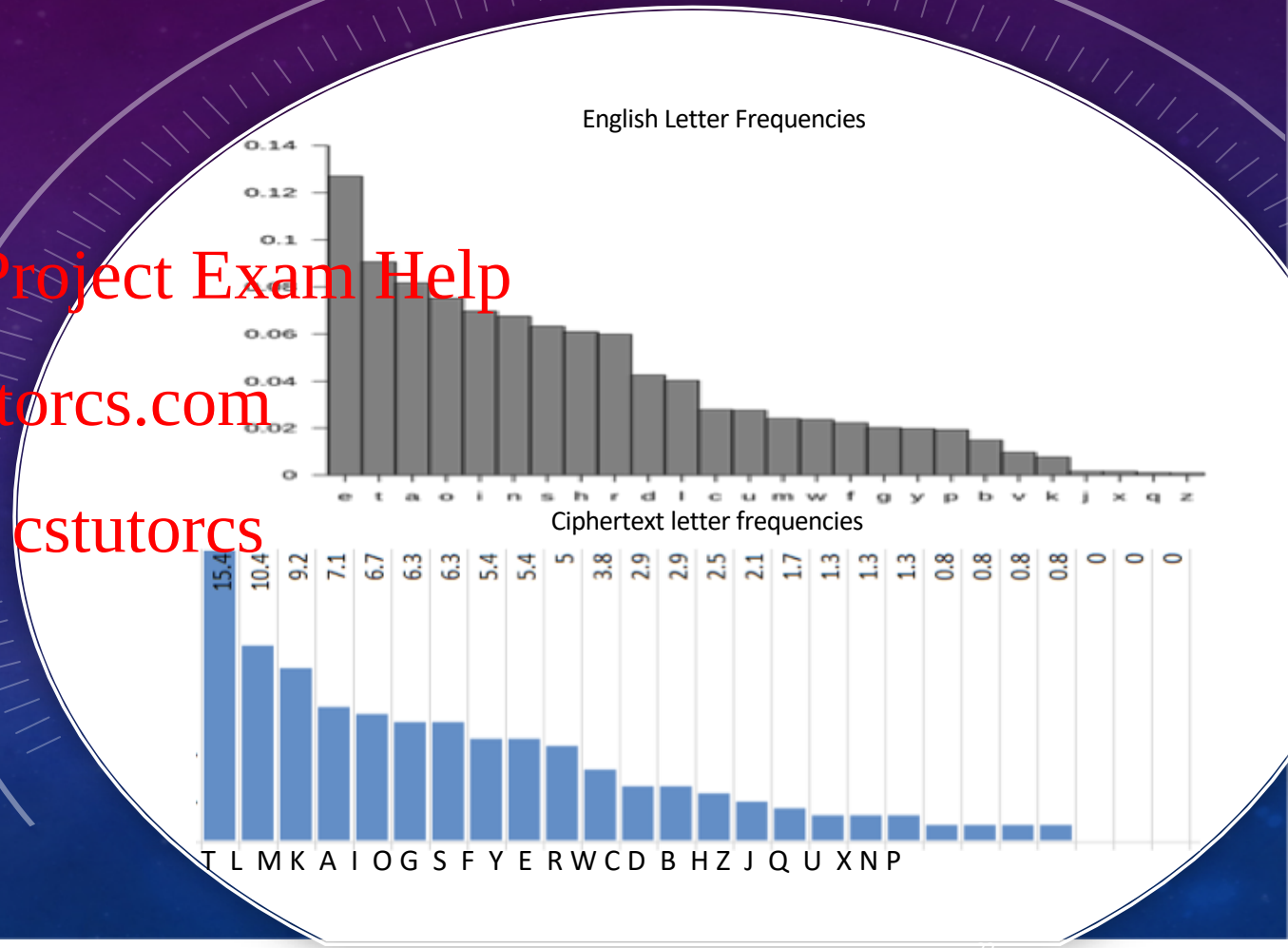
    as we'll see, they don't have to be too long!



FREQUENCY ANALYSIS ATTACK: EXAMPLE

Given the ciphertext:

```
STUTFR LIASS LHTAQ GY LAEKOYOET AM
CGKSRL TFR MIT COFR LAOSL GXTK MIT
CAMTKL LWKYAET JWOTMSB ZWM LWKTSB
TXTF OY MIT DGKKGC OL ZAKKTF GY
HKGDOLTL FGMIOFU LIASS YGKTLMASS DB
KTMWKF MG ZTEGDT MIT RTC MIAM
JWTFEITL MIT SAFR MG LHAKT MIT
LAFRL MIT LTAL MIT LQOTL O GYYTK
MITT MIOL LOSTFM LAEKOYOET
```



FREQUENCY ANALYSIS ATTACK: EXAMPLE

1. See the frequency table, replace T with E, because normally the letters with highest frequencies will match

```
SEUEFR LIASS LHEAQ GY LAEKOYOEE AM
CGKSRL EFR MIE COFR LAOSL GXEK MIE
CAMEKL LWKYAEE JWOEMSB ZWM LWKESB
EXEF OY MIE DGKKGC OL ZAKKEF GY
HKGDOLEL FGMIOFU LIASS YGKELMASS DB
KEMWKF MG ZEEGDE MIE REC MIAM
JWEFEIEL MIE SAFR MG LHAKE MIE
LAFRL MIE LEAL MIE LQOEL O GYYEK
MIEE MIOL LOSEFM LAEKOYOEE
```

2. See the replaced ciphertext, any short & repeated words? One short word that ends with E is THE. Update the table.

```
SEUEFR LHASS LHEAQ GY LAEKOYOEE AT
CGKSRL EFR THE COFR LAOSL GXEK THE
CATEKL LWKYAEE JWOETSB ZWT LWKESB
EXEF OY THE DGKKGC OL ZAKKEF GY
HKGDOLEL FGTHOFU LHASS YGKELTASS DB
KETWKF TG ZEEGDE THE REC THAT
JWEFEHEL THE SAFR TG LHAKE THE
LAFRL THE LEAL THE LQOEL O GYYEK
THEE THOL LOSEFT LAEKOYOEE
```


Ciphertext	Frequency	Plaintext
T	15.4	E
L	10.4	T
M	9.2	A
K	7.1	O
A	6.7	I
P	6.3	N
O	6.3	S
G	5.4	H
S	5.4	R
F	5	D
Y	3.8	L
E	2.9	C
R	2.9	U
W	2.5	M
C	2.1	W
D	1.7	F
B	1.3	G
H	1.3	Y
Z	1.3	P
J	0.8	B
Q	0.8	V
U	0.8	K
X	0.8	J
N	0	X
P	0	Q
V	0	Z

FREQUENCY ANALYSIS ATTACK: EXAMPLE

3. There are still short words e.g. “I”, “but”, can be guessed from current ciphertext. Replace Z with B, W with U, O with I.

```
SEUEFR LHASS LHEAQ GY LAEKIYIEE AT
CGKSRL EFR THE CIFR LAISL GXEK THE
CATEKL LUKYAEE JUIETSB BUT LUKESB
EXEF IY THE DGKKGC IL BAKKEF GY
HKGDILEL FGTHIFU LHASS YGKELTASS DB
KETUKF TG BEEGDE THE REC THAT
JUEFEHEL THE SAFR TG LHAKE THE
LAFRL THE LEAL THE LQIEL I GYYEK
THEE THIL LISEFT LAEKIYIEE
```

4. With the replaced ciphertext, we can discover even more short words, such as “that”, “to”, “if” and “this”. Notice that the plaintext of A is A too, which is not shown in the frequency analysis because the sample text is not long enough.

```
SEUEFR SHASS SHEAQ OF SAERIFIEE AT
CORSRS EFR THE CIFR SAISS OXER THE
CATERS SURFAEE JUIETSB BUT SURESB
EXEF IF THE DORROC IS BARREF OF
HRODISES FOTHIFU SHASS FORESTASS DB
RETURF TO BEEODE THE REC THAT
JUEFEHES THE SAFR TO SHARE THE
SAFRS THE SEAS THE SQIES I OFFER
THEE THIS SISEFT SAERIFIEE
```

Ciphertext	Frequency	Plaintext
T	15.4	E
L	10.4	T
M	9.2	A
K	7.1	O
A	6.7	I
J	6.3	N
O	6.3	S
G	5.4	H
S	5.4	R
F	5	D
Y	3.8	L
E	2.9	C
R	2.9	U
W	2.5	M
C	2.1	W
D	1.7	F
B	1.3	G
H	1.3	Y
Z	1.3	P
J	0.8	B
Q	0.8	V
U	0.8	K
X	0.8	J
N	0	X
P	0	Q
V	0	Z

FREQUENCY ANALYSIS ATTACK: EXAMPLE

5. Looking back to the frequency table we have, replace E with C.

```
SEUEFR SHASS SHEAQ OF SACRIFICE AT
CORSRS EFR THE CIFR SAISS OXER THE
CATERS SURFACE JUIETSB BUT SURESB
EXEF IF THE DORROC IS BARREF OF
HRODISES FOTHIFU SHASS FORESTASS DB
RETURF TO BECODE THE REC THAT
JUEFCHES THE SAFR TO SHARE THE
SAFRS THE SEAS THE SQIES I OFFER
THEE THIS SISEFT SACRIFICE
```

6. Continue with the table, skipping the letters that are already being replaced, replace C with W

```
SEUEFR SHASS SHEAQ OF SACRIFICE AT
WORSRS EFR THE WIFR SAISS OXER THE
WATERS SURFACE JUIETSB BUT SURESB
EXEF IF THE DORROW IS BARREF OF
HRODISES FOTHIFU SHASS FORESTASS DB
RETURF TO BECODE THE REW THAT
JUEFCHES THE SAFR TO SHARE THE
SAFRS THE SEAS THE SQIES I OFFER
THEE THIS SISEFT SACRIFICE
```


Ciphertext	Frequency	Plaintext
T	15.4	E
L	10.4	T
M	9.2	A
K	7.1	O
A	6.7	I
J	6.3	N
O	6.3	S
G	5.4	H
S	5.4	R
F	5	D
Y	3.8	L
E	2.9	C
R	2.9	U
W	2.5	M
C	2.1	W
D	1.7	F
B	1.3	G
H	1.3	Y
Z	1.3	P
J	0.8	B
Q	0.8	V
U	0.8	K
X	0.8	J
N	0	X
P	0	Q
V	0	Z

FREQUENCY ANALYSIS ATTACK: EXAMPLE

7. Ciphertext letter B has two possible plaintext letters, which is G and Y. Looking at the current text, the words containing B makes more sense if replacing with Y, thus replace B with Y.

```
SEUEFR SHASS SHEAQ OF SACRIFICE AT
WORSRS EFR THE WIFR SAISS OXER THE
WATERS SURFACE JUIETSY BUT SURESY
EXEF IF THE DORROW IS BARREF OF
HRODISES FOTHIFU SHASS FORESTASS DY
RETURF TO BECODE THE REW THAT
JUEFCHES THE SAFR TO SHARE THE
SAFRS THE SEAS THE SQIES I OFFER
THEE THIS SISEFT SACRIFICE
```

8. Using the same method as in Step 7, replace Q with K instead of V and J.

```
SEUEFR SHASS SHEAK OF SACRIFICE AT
WORSRS EFR THE WIFR SAISS OXER THE
WATERS SURFACE JUIETSY BUT SURESY
EXEF IF THE DORROW IS BARREF OF
HRODISES FOTHIFU SHASS FORESTASS DY
RETURF TO BECODE THE REW THAT
JUEFCHES THE SAFR TO SHARE THE
SAFRS THE SEAS THE SKIES I OFFER
THEE THIS SISEFT SACRIFICE
```


Ciphertext	Frequency	Plaintext
T	15.4	E
L	10.4	T
M	9.2	A
K	7.1	O
A	6.7	I
J	6.3	N
O	6.3	S
G	5.4	H
S	5.4	R
F	5	D
Y	3.8	L
E	2.9	C
R	2.9	U
W	2.5	M
C	2.1	W
D	1.7	F
B	1.3	G
H	1.3	Y
Z	1.3	P
J	0.8	B
Q	0.8	V
U	0.8	K
X	0.8	J
N	0	X
P	0	Q
V	0	Z

M
A
G
Q
L
I
K
W
Y
B
Z
Q

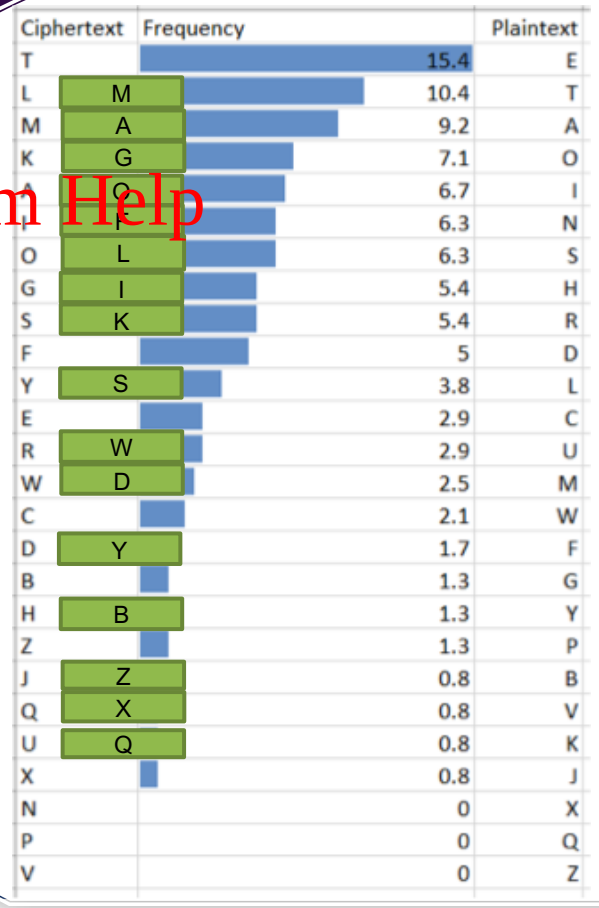
FREQUENCY ANALYSIS ATTACK: EXAMPLE

9. We can tell “shall”, “forestall”, “over”, “even”, “morrow”, replacing S with L, X with V, F with N, D with M respectively.

```
LEUENR SHALL SHEAK OF SACRIFICE AT
WORLRS ENR THE WINR SAILS OVER THE
WATERS SURFACE JUIETLY BUT SURELY
EVEN IF THE MORROW IS BARREN OF
HROMISES NOTHINU SHALL FORESTALL MY
RETURN TO BECOME THE REW THAT
JUENCHES THE LANR TO SHARE THE
SANRS THE SEAS THE SKIES I OFFER
THEE THIS SILENT SACRIFICE
```

8. Using same method as in Step 9, replace R with D, H with P, U with G…and the rest of the letters accordingly.

```
LEGEND SHALL SPEAK OF SACRIFICE AT
WORLDS END THE WIND SAILS OVER THE
WATERS SURFACE QUIETLY BUT SURELY
EVEN IF THE MORROW IS BARREN OF
PROMISES NOTHING SHALL FORESTALL MY
RETURN TO BECOME THE DEW THAT
QUENCHES THE LAND TO SPARE THE
SANDS THE SEAS THE SKIES I OFFER
THEE THIS SILENT SACRIFICE
```



FAILED ATTEMPT TO FIX THE MONOALPHABETIC STATISTICAL WEAKNESS

How about a more complex **two**–step cipher:

1. Encrypt message M with monoalphabetic key K1 to get ciphertext C1
2. Encrypt C1 again with monoalphabetic cipher with a different key K2 to get ciphertext C2

$$M \xrightarrow{K1} C1 \xrightarrow{K2} C2$$

Q: Is the two-step more secure than one-step monoalphabetic cipher?

A: No. Why?

Activity (5 mins)

1) Click the latest link in the Zoom chat
2) Add your question response to the Ed forum

Example III: Transposition Cipher: Rail Fence Cipher

Symmetric Crypto

- an example transposition cipher
- letters placed in multiple number of lines,
  from line 1 position 1 to line 2 position 2, then line 3 position 3, line 2 position 4,
  line 1 position 5, etc
- e.g. the plaintext **"WE ARE DISCOVERED FLEE AT ONCE"**

  W . . . E . . . C . . . R . . . L . . . T . . . E

  . E . R . D . S . O . E . E . F . E . A . O . C .

  . . A . . . I . . . V . . . D . . . E . . . N . .
- ciphertext: **wecrlte erdsoeefeaoc aivden**

- Q: What is the key for this example of rail fence cipher?
- **Rail fence of depth 3**

Example III: Transposition Cipher: General

Symmetric Crypto

- Decide on a block size L (say L = 10 letters)
- Fix a permutation of (0,1,2,3,…,9) i.e. the key K:
  - e.g. K = (**5**,3,1,4,6,8,2,0,9,7)
  - Transpose every block of L successive message letters according to K, e.g.:

```
                0123456789 0123456789
  Message = HELLOTHERE HOWARETHEY
  Cipher  = TLEOHRLHEE EAORTEEWHY
```

- Secure?
  - No – Statistical patterns (letter frequencies) remain in ciphertext!

MONASH University

Encryption: Modern Cipher principles

Modern Ciphers = Product Ciphers

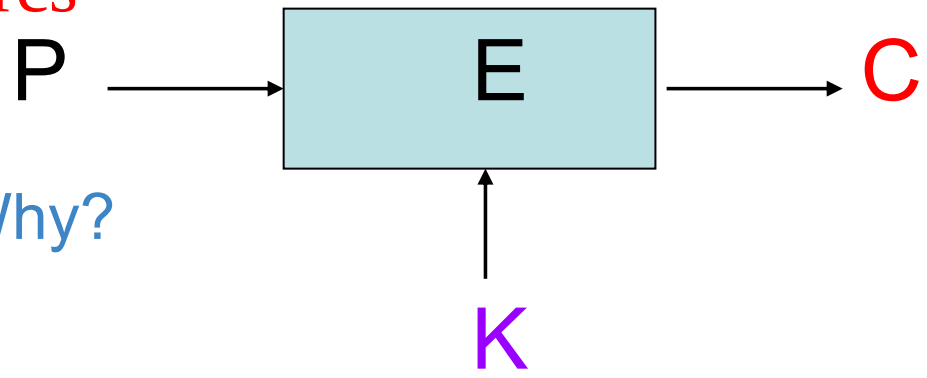
Symmetric Crypto

- Substitution & Transposition
  - each contributes own strength to encryption
- Q: does combining a monoalphabetic substitution & transposition cipher give a
  - Monoalphabetic substitution cipher?
  - A transposition cipher?
- No! product is more complex than either one individually!
  - Number of possible product keys is (likely to be) the product of number of keys of individual methods

Cipher Properties (I)

Symmetric Crypto

- **Confusion**
  - make the **relationship** between ciphertext C & encryption key K as **complex as possible**
    - otherwise observing C statistics would leak info on K
  - achieved by **complex substitution**
  - **Hard to get** K by **observing** C

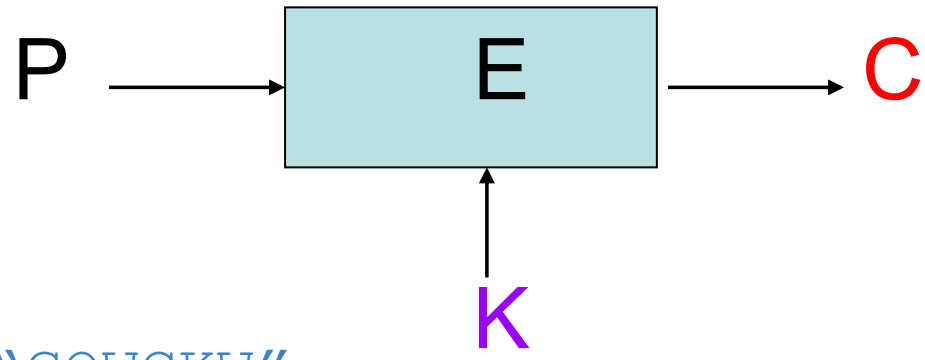


Q: Does Caesar cipher have confusion? Why?

Cipher Properties (II)

Symmetric Crypto

- **Diffusion**
  - should **spread** the information from P so that (eventually) each P digit affects many C digits
  - achieved by complex **transposition**
  - patterns in P can no longer be observed in C



  - Q: If some cipher encrypts P="HE**L**PME" to C="GQWCKW"
  - and encrypts P="HE**M**PME" to C="GQADKW"
  - Does this cipher achieve Diffusion? Why/why not?

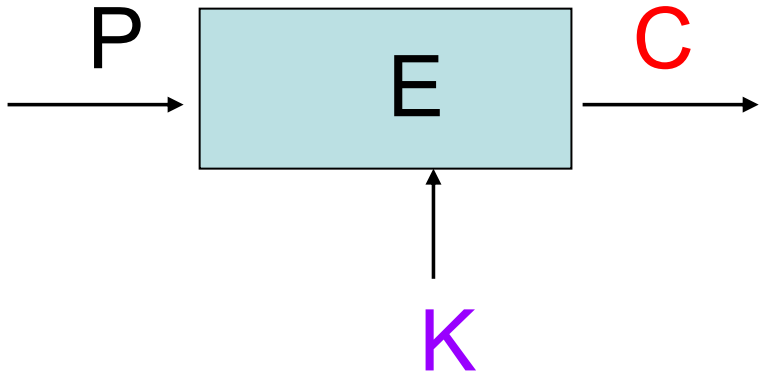
Activity (5 mins)
Add your question response to the Ed forum

Cipher Properties (III)

Symmetric Crypto

- **Avalanche effect (diffusion for changes in either P or K)**
  - Small change in either plaintext P or key K produces a **significant** change in the ciphertext C
    - E.g. change in one bit of P or one bit of K should produce a change in **many bits** of C

- E.g.
- `P=11000000, K = 01101101 → C = 10101011`
- `P=11000000, K = 01111101 → C = 11011101`



Unconditional vs Computational Security

Symmetric Crypto

- **Two kinds of encryption security requirements**

- **Unconditional** security / information-theoretic security
  - even if attacker has infinite computational power,
    - cannot get information on plaintext from ciphertext

- **Computational** security
  - if attacker has limited computational power,
    - cannot get information on plaintext from ciphertext
    - time needed for attack > useful age of info
    - cost of breaking > value of info

The One-Time Pad

Symmetric Crypto

- **Q: Is unconditionally secure encryption possible?**
- **A: Yes - One-Time Pad Encryption**
  - start with the Caesar substitution cipher
  - but use an independent random alphabet shift for for each plaintext letter:

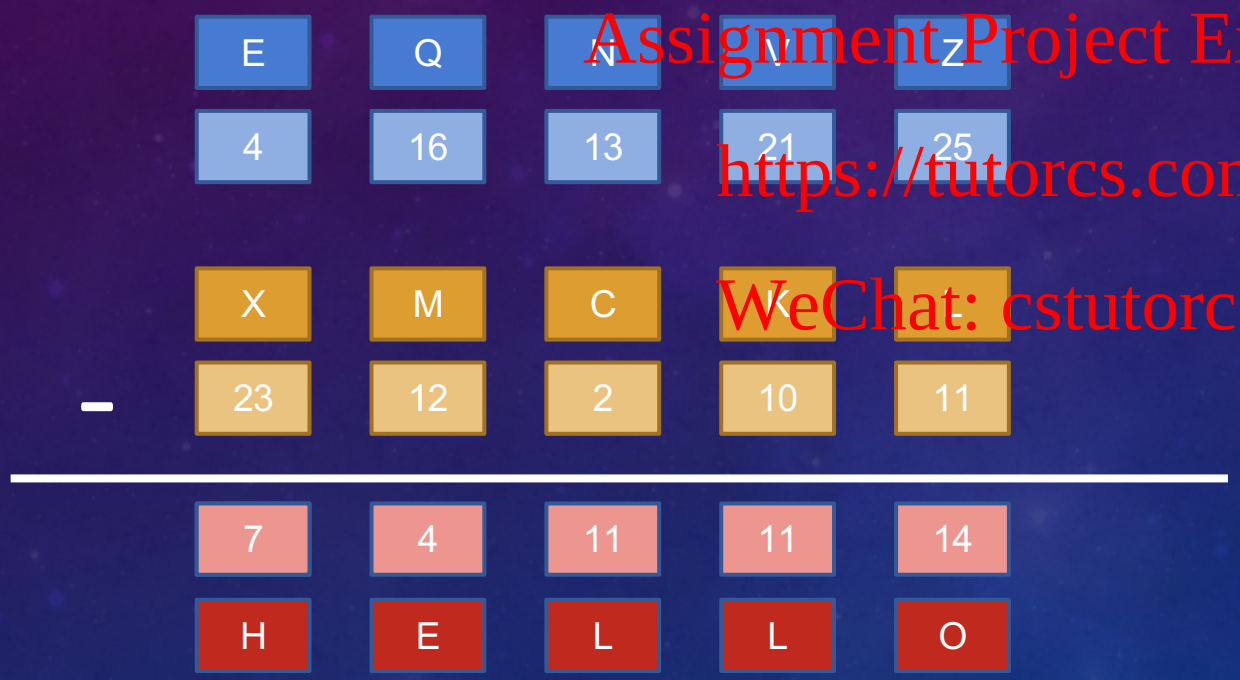
e.g.

```
K = (2,9,13,20,4)
M =  H E  L  L  O
C =  J N  Y  F  P
```

- Claim: It is not possible to break this cipher by brute force exhaustive search. Q: **Why**?

EXAMPLE OF DECRYPTING ONE-TIME PAD BY USING RANDOM KEY

Given a ciphertext “EQNVZ”. Assume we already obtained the random key, which is also the same length “XMCKL”, how do we decrypt the message?



1. Convert the letters into numbers, where A = 0, B = 1…Z = 25

2. Subtract the value of random key from the ciphertext

3. If the result is a negative number, calculate how much it needs to reach 26. In this case, -19-7 = -26. Thus 7.

4. Convert the number back into alphabets, which is the message in plaintext

ONE-TIME PAD USING RANDOM KEY

IMPOSSIBLE TO APPLY BRUTE FORCE ATTACK!

Why is brute force attack impossible on a one-time pad?

Reason is NOT the complexity of brute force!

e.g. a short plaintext “Alice”, we will have 26*26*26*26*26 = 11,881,376 possibilities, which is easy to search through in a fraction of a second on any computer today

However if we are using random key for each of the alphabet, this is like rolling a 26-sided die for each encrypted letter

REASON FOR IMPOSSIBILITY TO BRUTE FORCE THE ONE-TIME PAD: ALL POSSIBLE DECRYPTIONS ARE EQUALLY LIKELY

It is possible to brute force the number of possibilities in previous slide.

However, since each possible key is equally likely, it is impossible to know which decryption is the correct one, i.e.

All possible English words with the same length as the ciphertexts are possible decryptions!

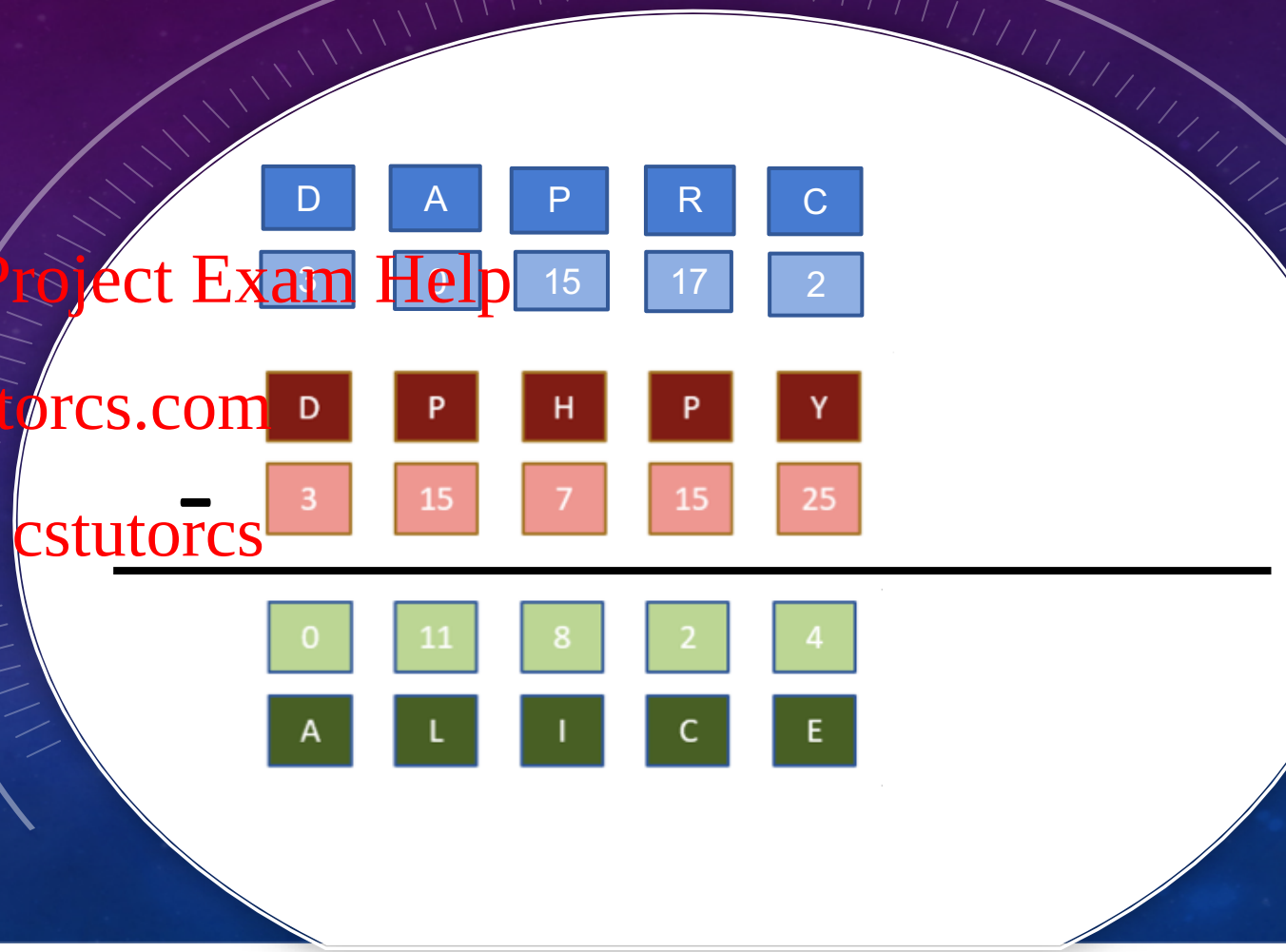
E.g. Ciphertext = “DAPRC”

and 3 different possible keys:

Key 1: WWEGO

Key 2: QACPE

Key 3: DPHPY



One-Time Pad: Why not popular?

Symmetric Crypto

- Big Problem: Key is as long as the message…
  - leads to impractical key exchange problem for most (large) messages

- However, still used for **very high security** applications
  - e.g. (famous historical example): White-House to Kremlin nuclear emergency "hotline" (red telephone): *keying tapes physically delivered via embassy*

Security in practice: Computational security

Symmetric Crypto

- via Substitution-Transposition Product Cipher
- Substitution:
  - need to exchange & remember the substitution table
  - table can be big, if alphabet size is large
- Transposition/Permutation:
  - plaintext is rearranged i.e. **permutation**
- Design principles
  - Need to avoid large substitution tables, but still need a method to substitute characters (or bits)
  - Need efficient permutation/transposition method