ECE458/ECE750T27: Computer Security

Cryptography

Dr. Kami Vaniea
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
    1. Some students show up late for various good reasons
    2. Reward students who show up on time
    3. Important to see real world examples

How do I turn on the Do Not Track feature?

Firefox **Last updated:** 2/21/25 **65%** of users voted this helpful

---

Starting in Firefox version 135, the "Do Not Track" setting has been removed. Many sites do not respect this indication of a person's privacy preferences and, in some cases, it can reduce privacy. If you wish to ask websites to respect your privacy, you can use the "Tell websites not to sell or share my data" setting built on top of the Global Privacy Control (GPC) feature. GPC is respected by increasing numbers of sites and enforced with legislation in some regions. To learn more, please read Global Privacy Control.

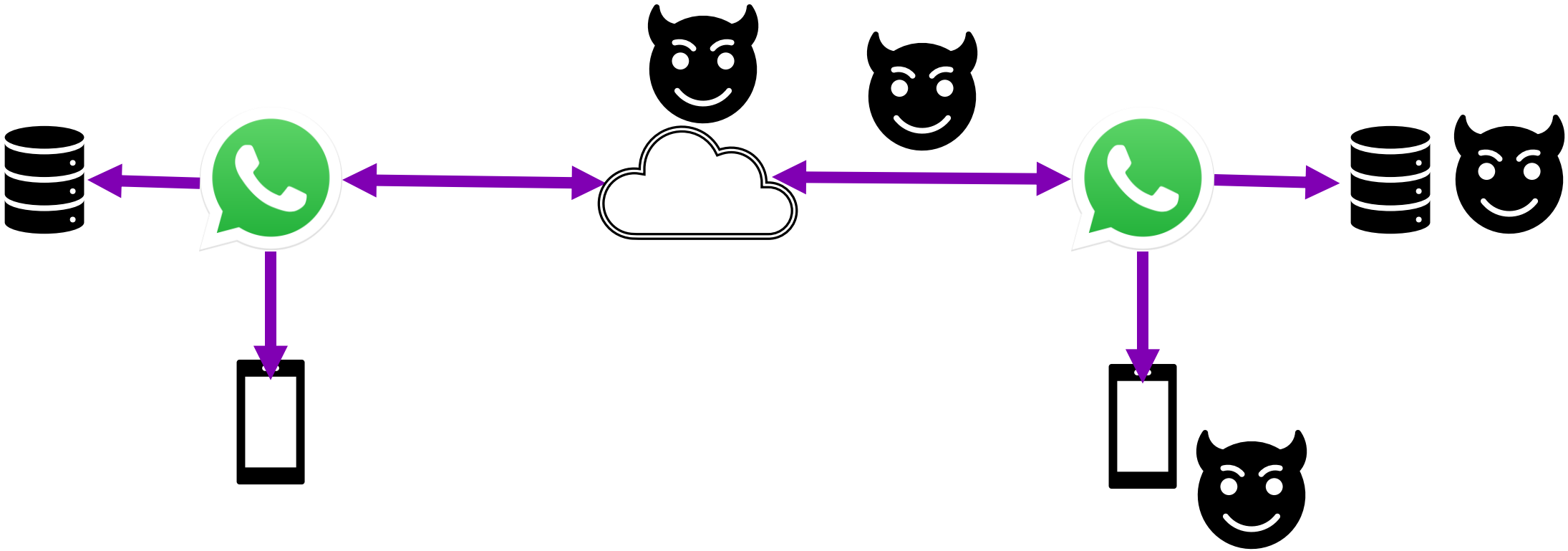
Related Courses and Opportunities

- ECE 499 - Project Course
- ECE 409 - Cryptography and System Security
- Computer Science Security Courses:
  - https://crysp.uwaterloo.ca/courses/

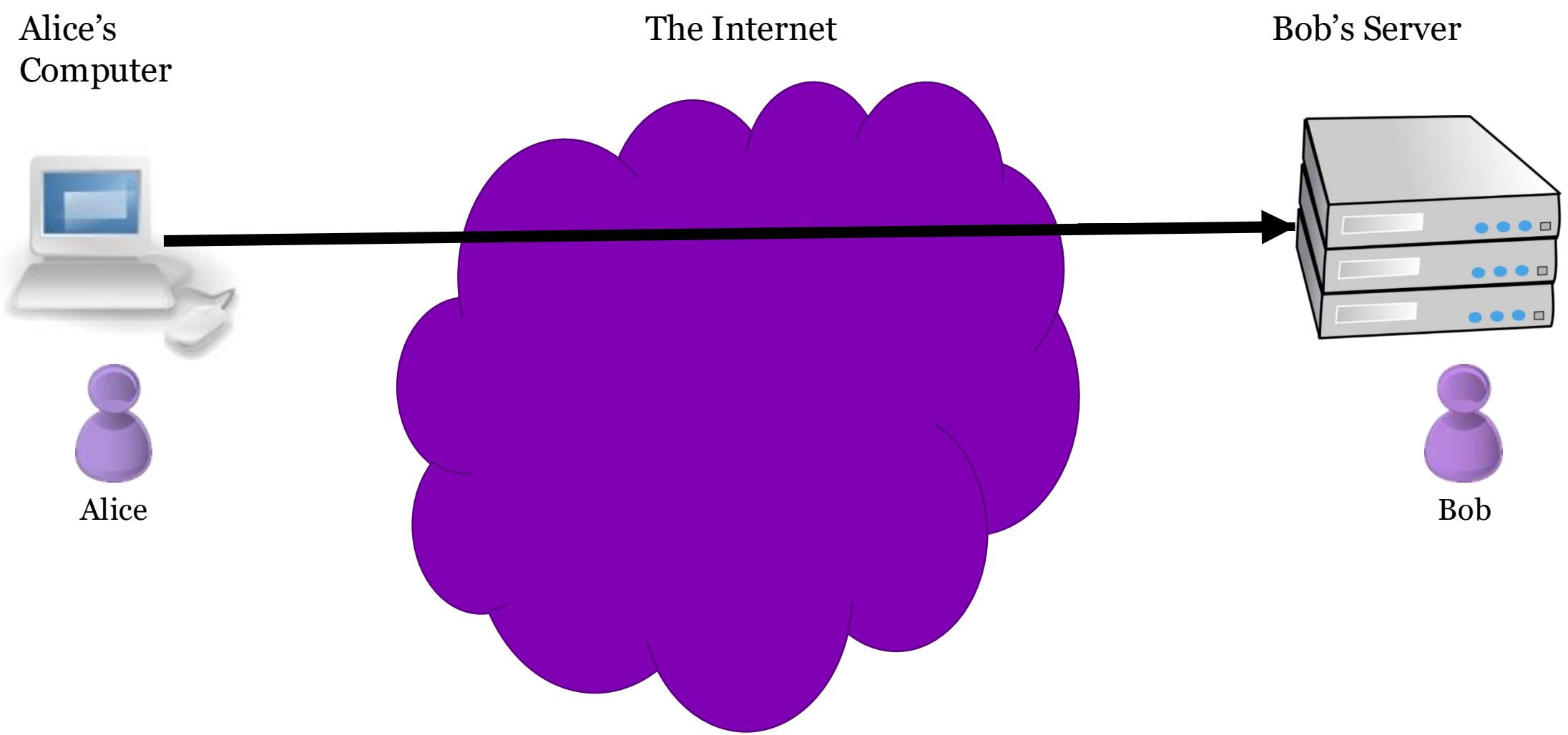
Online Courses

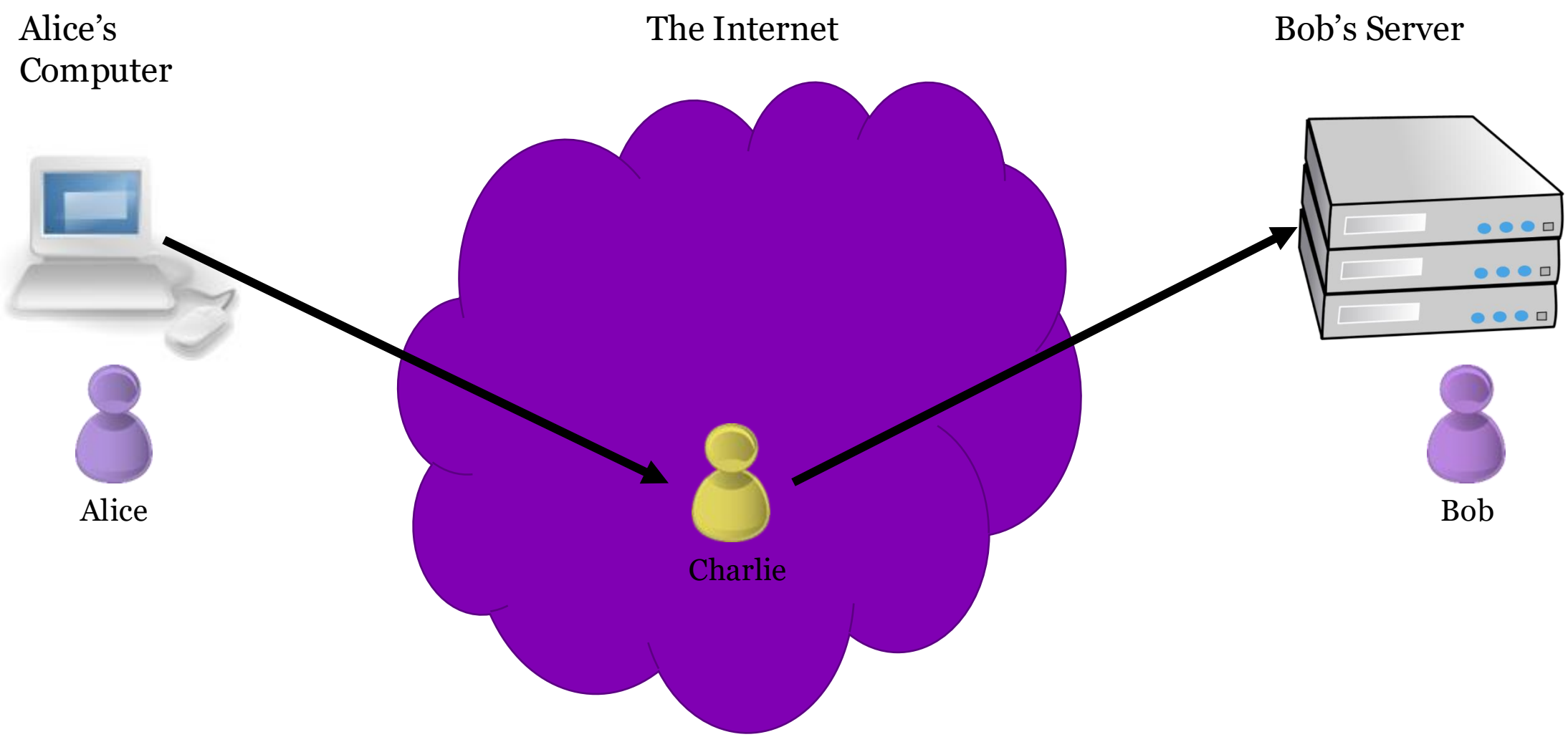
- Cryptography 101 with Alfred Menezes - https://cryptography101.ca/

Data exists in different places, and the approaches to protect it differ depending on where it is.



MAN IN THE MIDDLE ATTACK

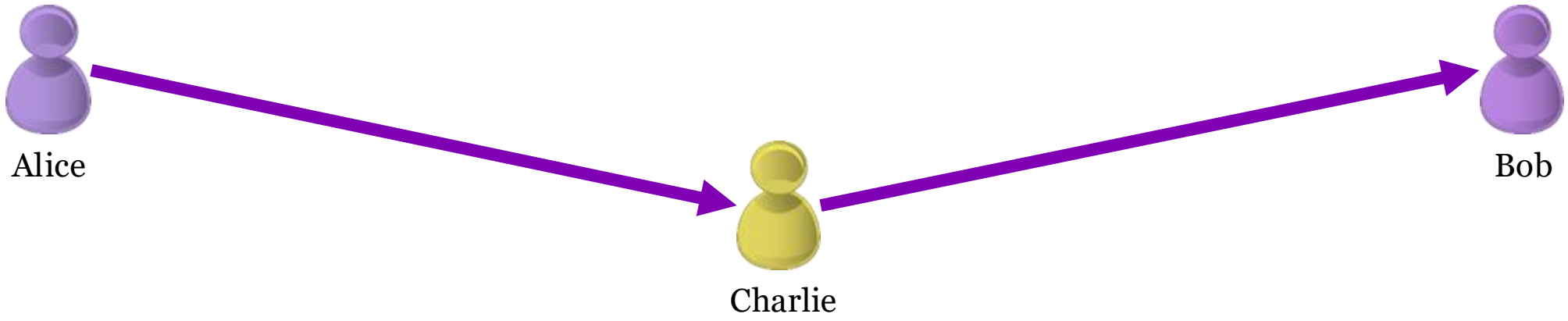

Alice's Computer
The Internet
Bob's Server
Alice
Bob


Alice's Computer
The Internet
Bob's Server
Alice
Charlie
Bob

Charlie is in the middle between Alice and Bob.

- Charlie can:
  - View (confidentiality)
  - Change (integrity)
  - Add (integrity)
  - Delete (integrity, availability)

- Charlie could be:
  - Internet service provider
  - Virtual Private Network (VPN) provider
  - WIFI provider such as a coffee shop
  - An attacker re-routing your connection
  - An incompetent admin (it happens)



Man in the middle attacks happen all the time and they are not always bad.

Alice goes to her favorite coffee shop and tries to visit BBC News

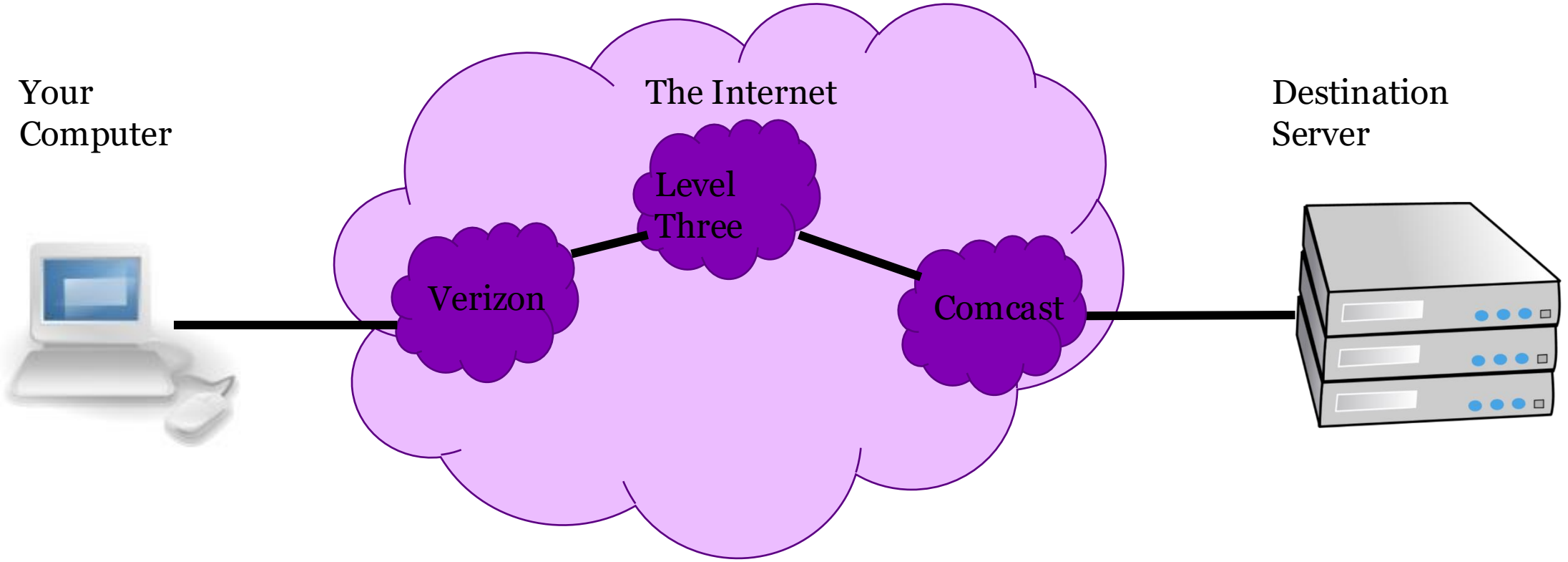
Alice

Alice

BBC NEWS


I'm Feelin
STARBUCKS
Google
WIFI
Free Wi-Fi
From our friends at Google
Accept & Connect
I agree to the Terms of Service and have reviewed the Google Privacy Policy
Need help? 855-446-2374
¡HOLA
GOOD MORNING
Google


Alice
Free Wi-Fi
Accept & Connect
Google
BBC
NEWS
STARBUCKS
COFFEE


Your
Computer
The Internet
Level
Three
Verizon
Comcast
Destination
Server

All the web servers contacted between my computer on UWaterloo campus and my lab's webserver hosted by Dreamhost in the USA.

```
tracepath tulipslab.org
 1?: [LOCALHOST]                      pmtu 1500
 1:  v1040-wn-rt-a.ns.uwaterloo.ca                          3.259ms
 1:  v1040-wn-rt-a.ns.uwaterloo.ca                          3.137ms
 2:  po101-40-4140-wn-rt.ns.uwaterloo.ca                    6.981ms
 3:  v1055-wn-rt.ns.uwaterloo.ca                            3.439ms
 4:  po40-dist-rt.ns.uwaterloo.ca                           3.528ms
 5:  po30-cn-rt.ns.uwaterloo.ca                             3.619ms
 6:  po100-cn-rt.ns.uwaterloo.ca                            8.563ms
 7:  hu-0-0-0-8-ext-rt-rac.ns.uwaterloo.ca                  6.300ms
 8:  unallocated-static.rogers.com                          8.209ms
 9:  unallocated-static.rogers.com                          5.846ms asymm  8
10:  24.156.146.189                                        14.307ms asymm  9
11:  209.148.235.214                                       10.922ms
12:  209.148.235.214                                       12.665ms asymm 11
13:  zayo.ip4.torontointernetxchange.net                   13.930ms asymm 12
14:  ae5.mpr1.tor3.ca.zip.zayo.com                         14.053ms asymm 13
15:  no reply
16:  ae24.mpr4.pdx1.us.zip.zayo.com                        63.631ms
17:  ae24.mpr4.pdx1.us.zip.zayo.com                        63.429ms asymm 16
18:  ae13.mpr2.pdx1.us.zip.zayo.com                        65.792ms asymm 17
19:  pdx1-cr-1.sd.dreamhost.com                            71.918ms asymm 22
20:  pdx1-cr-1.sd.dreamhost.com                            72.363ms asymm 22
```

Verizon MITMed traffic and added cookies to all connections so that advertisers could track better and link data to demographics Verizon provided.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BIZ & IT —

Verizon's zombie cookie gets new life

Verizon's tracking supercookie joins up with AOL's ad tracking network.

JULIA ANGWIN AND JEFF LARSON, PROPUBLICA - 10/7/2015, 8:00 AM

65

Verizon is giving a new mission to its controversial hidden identifier that tracks users of mobile devices. Verizon said in a little-noticed announcement that it will soon begin sharing the profiles with AOL's ad network, which in turn monitors users across a large swath of the Internet.

FURTHER READING
Verizon will now let users kill previously indestructible tracking code

That means AOL's ad network will be able to match millions of Internet users to their real-world details gathered by Verizon, including "your gender, age range and interests." AOL's network is on 40 percent of websites, including on ProPublica.

AOL will also be able to use data from Verizon's identifier to track the apps that mobile users open, what sites they visit, and for how long. Verizon purchased AOL earlier this year.

Aspidistra radio used by the UK in WWII. It re-broadcast German radio programs and occasionally added its own. By copying real broadcasts it seemed legitimate and was even used by the German military as a source of information.

On-device MITM Attack

Lenovo shipped computers with software that used MITM to inject ads into all network traffic.

ars TECHNICA

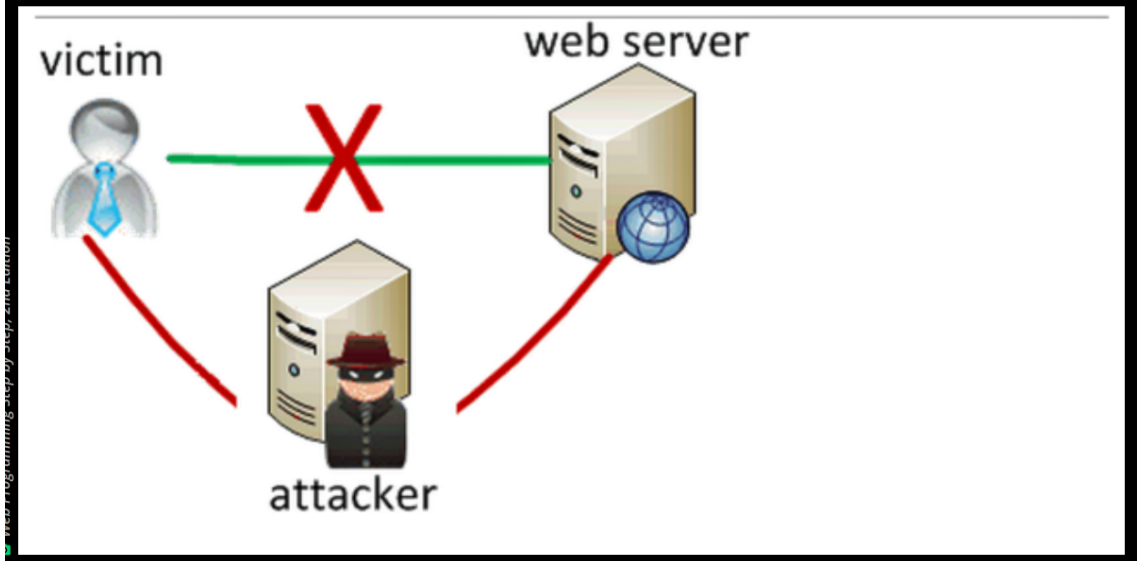
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BIZ & IT —

Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

DAN GOODIN - 2/19/2015, 11:36 AM



333

Lenovo is selling computers that come preinstalled with adware that hijacks encrypted Web sessions and may make users vulnerable to HTTPS man-in-the-middle attacks that are trivial for attackers to carry out, security researchers said.

The critical threat is present on Lenovo PCs that have adware from a company called Superfish installed. As unsavory as many people find software that injects ads into Web pages, there's something much more nefarious about the Superfish package. It installs a self-signed root HTTPS certificate that can intercept encrypted traffic for every website a user visits. When a user visits an HTTPS site, the site certificate is signed and controlled by Superfish and falsely represents itself as the official website certificate.

Even worse, the private encryption key accompanying the Superfish-signed Transport Layer Security certificate appears to be the same for every Lenovo machine. Attackers may be able to use the key to certify imposter HTTPS websites that masquerade as Bank of America, Google, or any other secure destination on the Internet. Under such a scenario, PCs that have the Superfish root certificate installed will fail to flag the sites as forgeries—a failure that completely undermines the reason HTTPS protections exist in the first place.

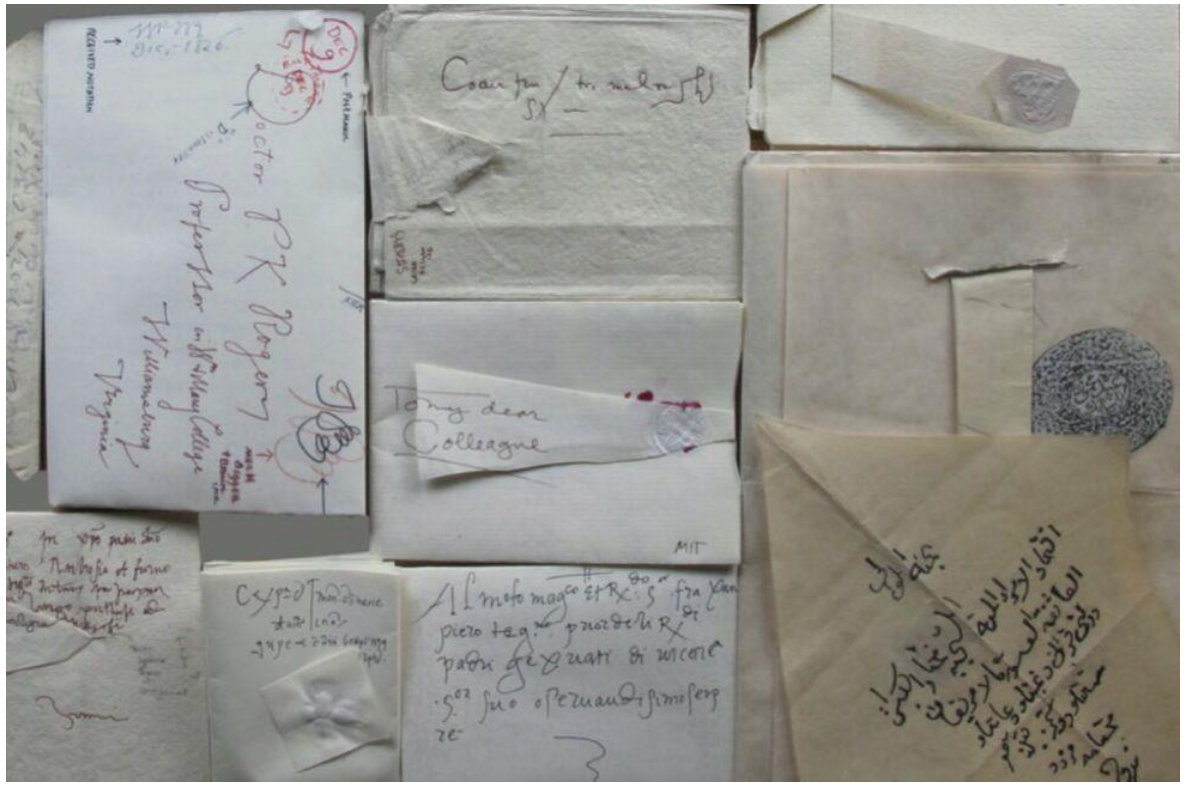
CRYPTOGRAPHY A MINI HISTORY

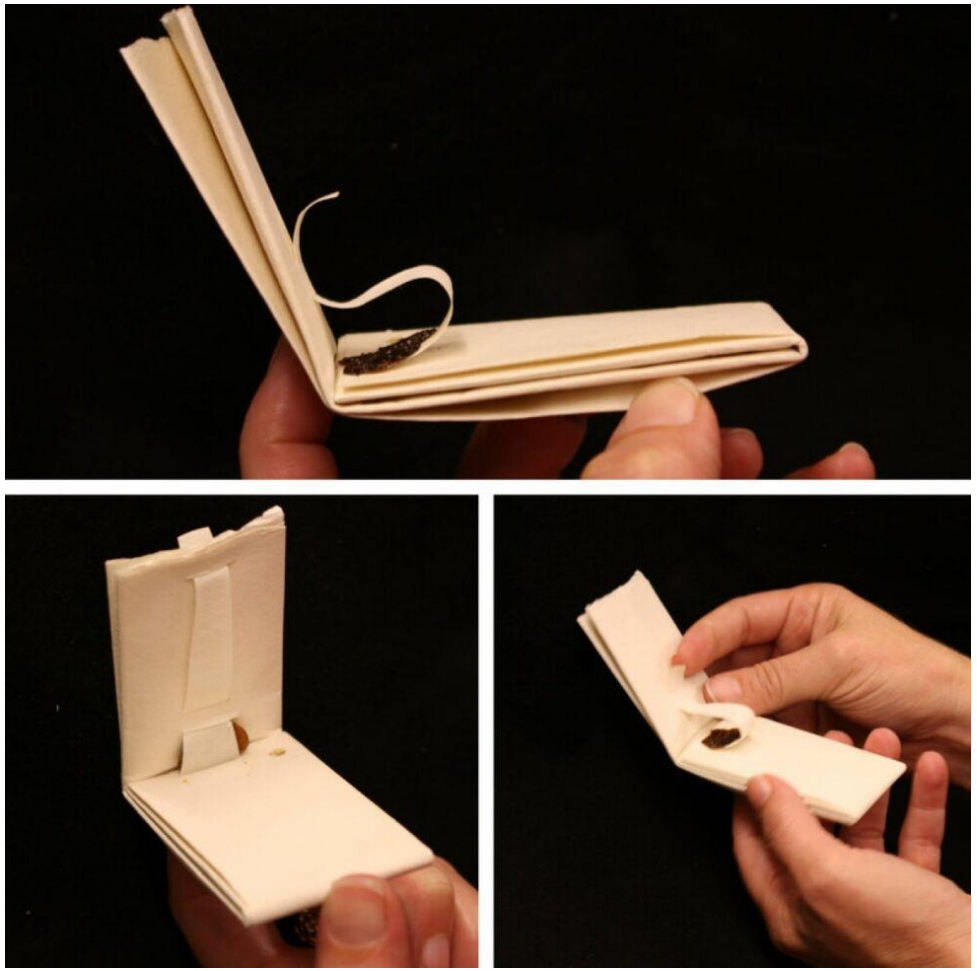
Cryptography refers to the science and art of designing ciphers; *cryptanalysis* to the science and art of breaking them; while *cryptology*, often shortened to just crypto, is the study of both.

-- Ross Anderson, Security Engineering

Letter Locks

Intricately folded letters use a type of physical cryptography to keep letters secure. Slips of paper are inserted and sealed with wax, impossible to open without tearing the paper.





https://arstechnica.com/science/2021/03/locked-for-300-years-virtual-unfolding-has-now-revealed-this-letters-secrets/

Cryptography

- Encryption is the process of encoding a message so that its meaning is not obvious. Also "encode" or "encipher"
- Decryption is the reverse process of transforming an encrypted message back into its normal original form. Also "decode" or "decipher"

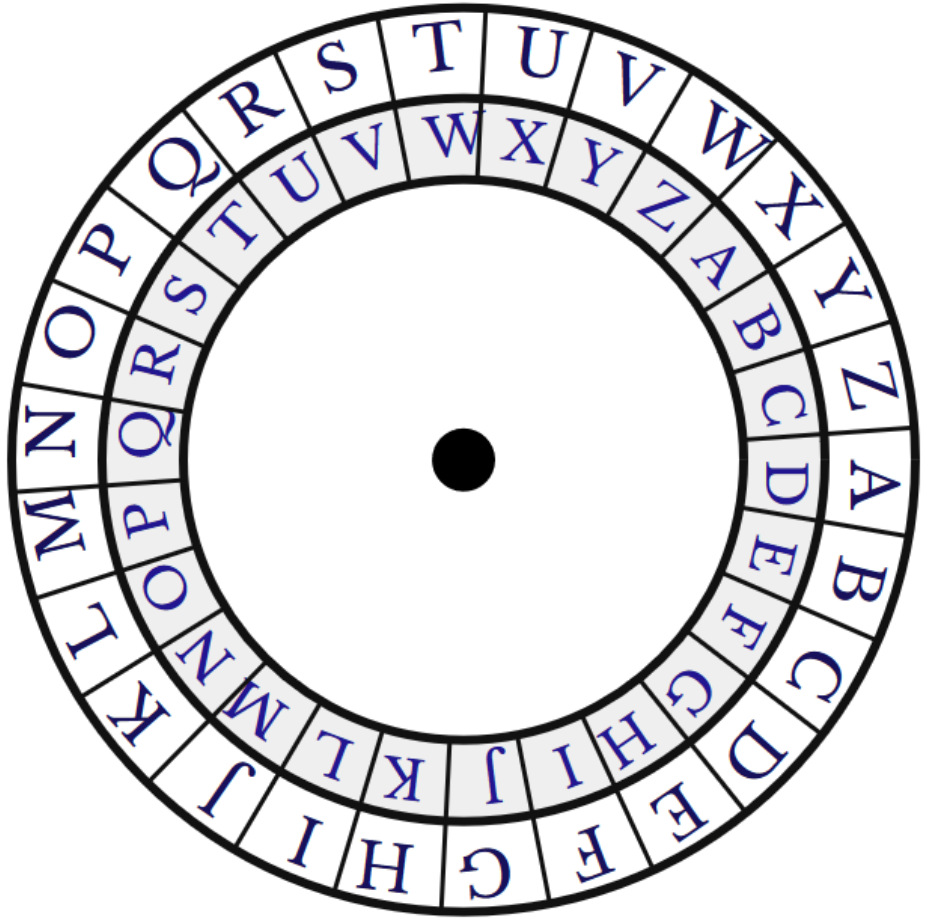
More formally:

- Encryption: C = E(K, P)
- Decryption: P = D(K, C)

- **C**iphertext, **P**laintext, **E**ncryption rule, **D**ecryption rule, **K**ey

Caesar Cipher

- In a Caesar Cipher (right) the “secret” is how many places to turn the wheel
- Encryption is done by finding a letter on the outer wheel and then writing down the letter on the inner wheel.
- Easy to break using modern computers by just guessing all 26 possibilities.



Overly simple example using Caesar Cipher with key 3:

Plain Text	**C**	**R**	**Y**	**P**	**T**	**O**
Cypher Text	F	U	V	S	E	R

https://www.xarg.org/tools/caesar-cipher/

Monoalphabetic Substitution

- Each letter of the alphabet directly corresponds to another letter.
- There is a range of ways to create maps.
- Easy to break though using frequency calculations since some letters occur more often than others.
- In English the most common letters are e,t,a,i,o,n,s,h,r,d,l,u in that order

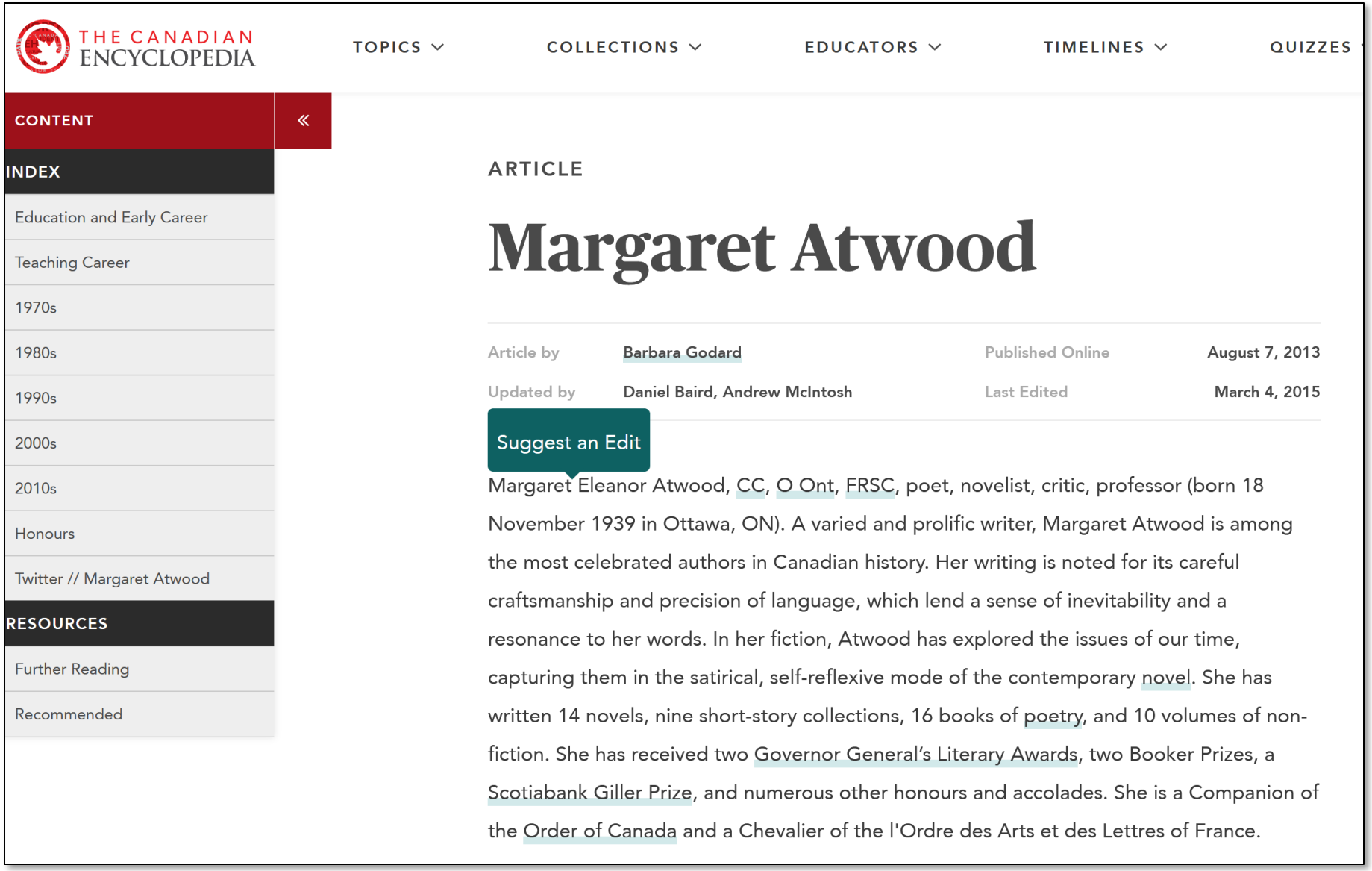
- Many approaches. For example, using a keyword and moving all those letters to the start.

```
alphabet  abcdefghijklmnopqrstuvwxyz
key       SECURITYABDFGHJKLMNOPQVWXZ
```

Plain Text	**C**	**R**	**Y**	**P**	**T**	**O**
Cypher Text	C	M	X	K	O	J

Substitution ciphers have a key weakness: frequency analysis.

Example: Text on Margaret Atwood



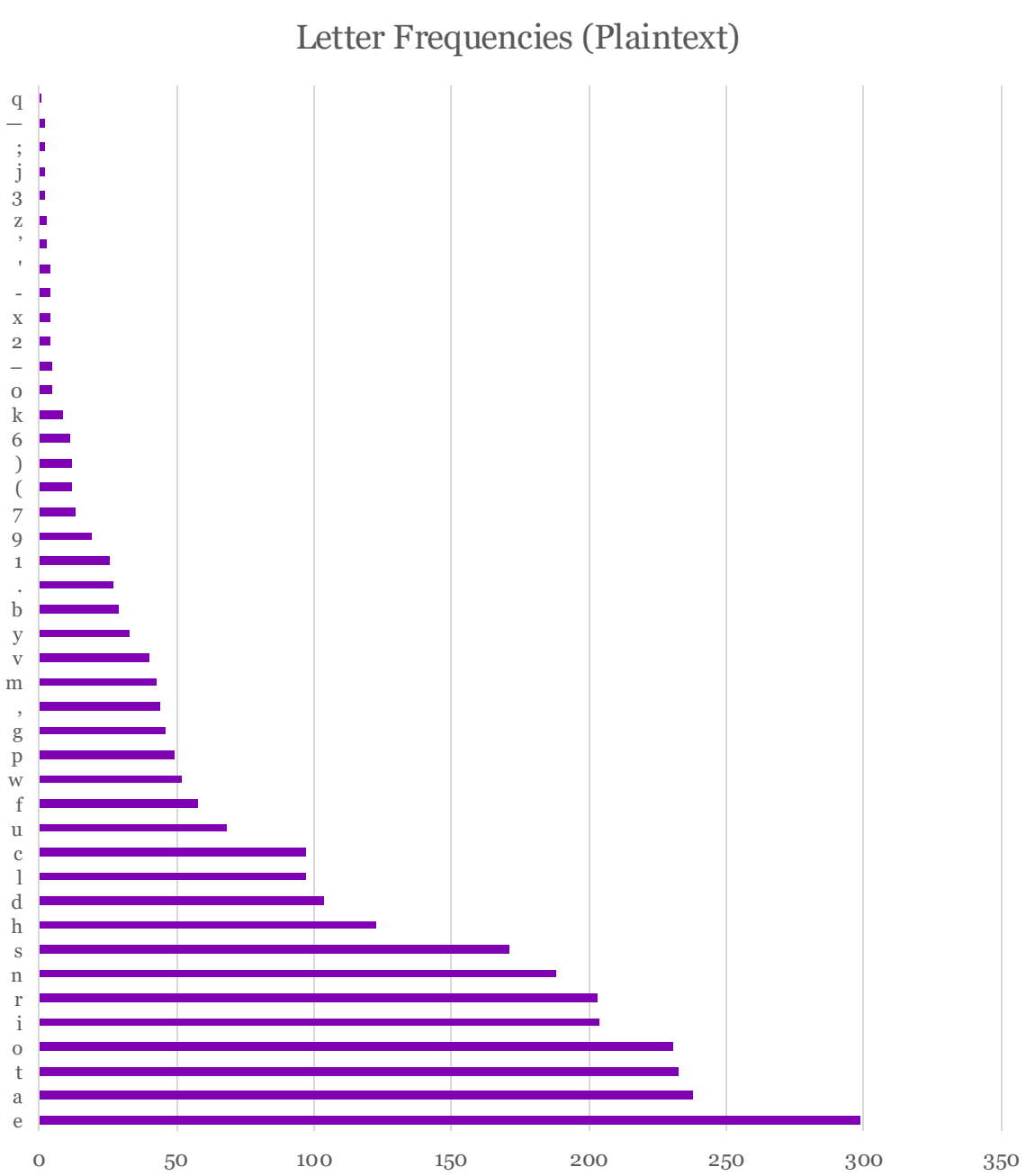
Caesar Cipher, shift 7 (a->h)

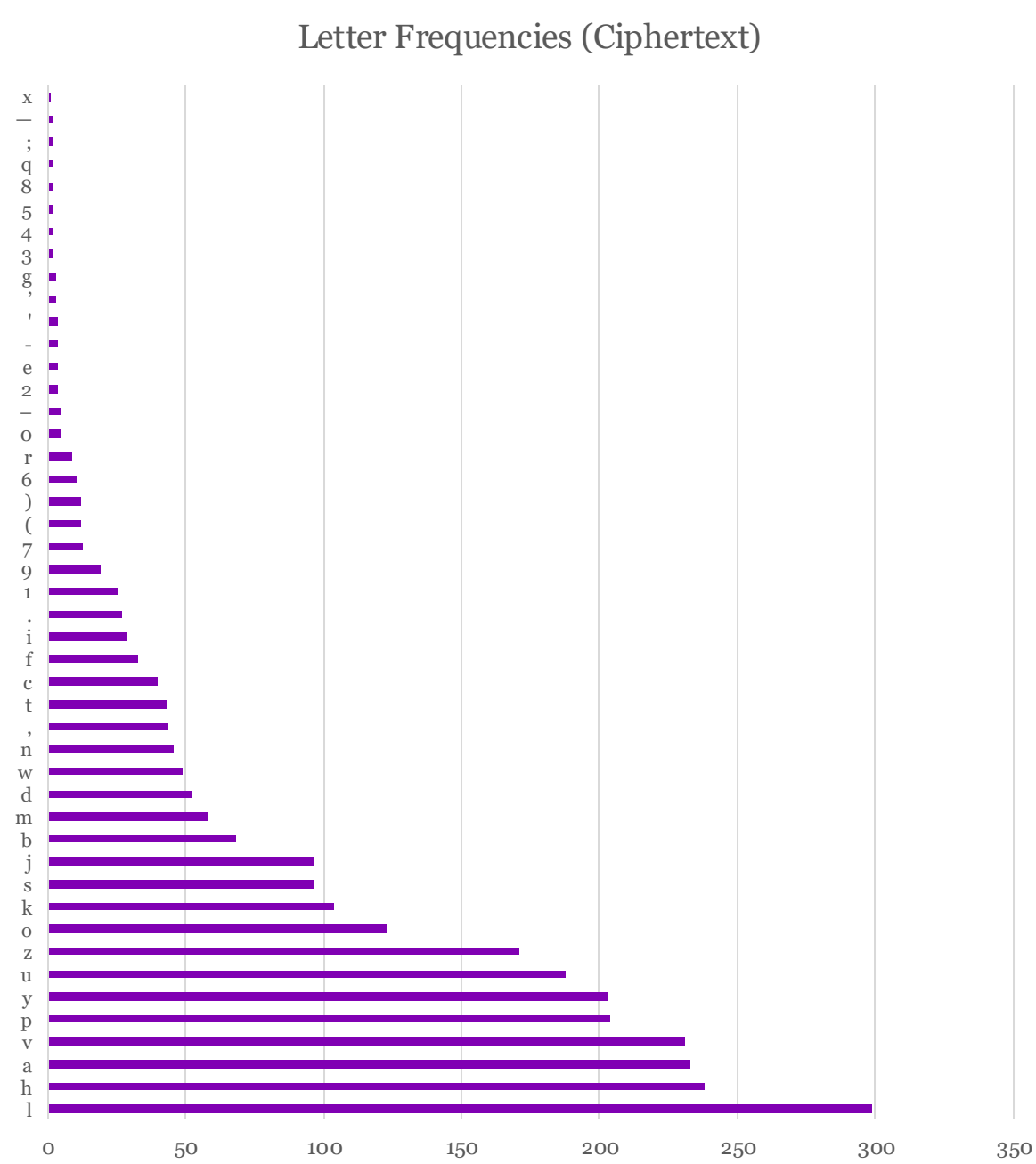
Plaintext

margaret eleanor atwood, cc, o ont, frsc, poet, novelist, critic, professor (born 18 november 1939 in ottawa, on). a varied and prolific writer, margaret atwood is among the most celebrated authors in canadian history. her writing is noted for its careful craftsmanship and precision of language, which lend a sense of inevitability and a resonance to her words. in her fiction, atwood has explored the issues of our time, capturing them in the satirical, self-reflexive mode of the contemporary novel. she has written 14 novels, nine short-story collections, 16 books of poetry, and 10 volumes of non-fiction. she has received two governor general's literary awards, two booker prizes, a scotiabank giller prize, and numerous other honours and accolades. she is a companion of the order of canada and a chevalier of the l'ordre des arts et des lettres of france.

Ciphertext

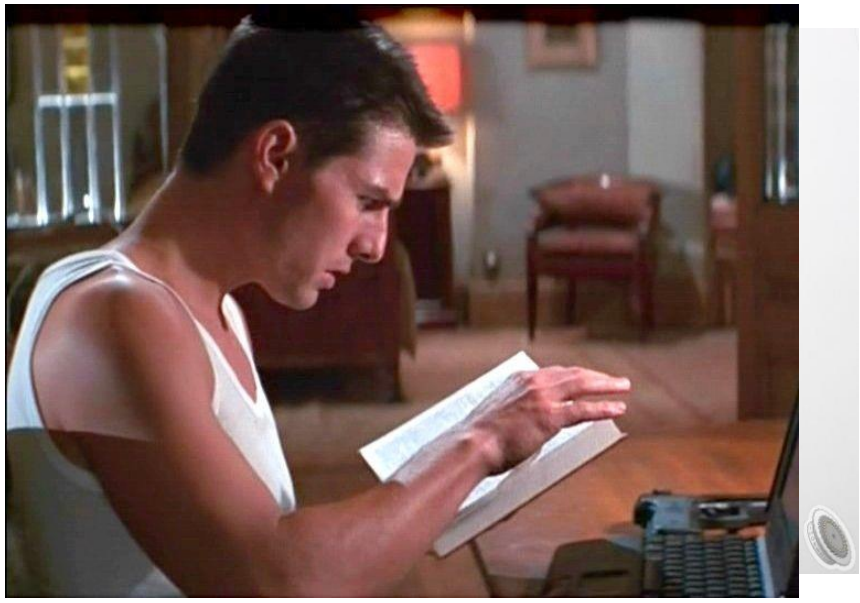
thynhyla lslhuvy hadvvk, jj, v vua, myzj, wvla, uvclspza, jypapj, wyvmlzzvy (ivyu 18 uvcltily 1939 pu vaahdh, vu). h chyplk huk wyvspmpj dypaly, thynhyla hadvvk pz htvun aol tvza jlsliyhalk hbaovyz pu jhuhkphu opzavyf. oly dypapun pz uvalk mvy paz jhylmbs jyhmazthuzopw huk wyljpzpvu vm shunbhnl, dopjo sluk h zluzl vm pulcpahipspaf huk h ylzvuhujl av oly dvykz. pu oly mpjapvu, hadvvk ohz lewsvylk aol pzzblz vm vby aptl, jhwabypun aolt pu aol zhapypjhs, zlsm-ylmslepcl tvkl vm aol jvualtwvyhyf uvcls. zol ohz dypaalu 14 uvclsz, upul zovya-zavyf jvssljapvuz, 16 ivvrz vm wvlayf, huk 10 cvsbtlz vm uvu-mpjapvu. zol ohz yljlpclk adv nvclyuvy nlulyhs'z spalyhyf hdhykz, adv ivvrly wypglz, h zjvaphihur npssly wypgl, huk ubtlyvbz vaoly ovuvbyz huk hjjvshklz. zol pz h jvtwhupvu vm aol vykly vm jhuhkh huk h jolchsply vm aol s'vykyl klz hyaz la klz slaaylz vm myhujl.


Letter Frequencies (Plaintext)
q — ; j 3 z ’ ' - x 2 – o k 6) (7 9 1 . b y v m , g p w f u c l d h s n r i o t a e
0 50 100 150 200 250 300 350


Letter Frequencies (Ciphertext)
x — ; q 8 5 4 3 g ’ ' - e 2 – o r 6) (7 9 1 . i f c t , n w d m b j s k o z u y p v a h l
0 50 100 150 200 250 300 350

One-time-pad

- Share a “key” in advance. Secret and fully random.
- Use the “key” to encrypt/decrypt by adding the letters.
  - C = P+K mod 26
- Each letter gets a number: A=0, B=1 …
- Add the numbers (mod 26) to encrypt, subtract (mod 26) to decrypt
- One of the strongest forms of encryption.
- But… you have to pre-share keys that are as long as the plain text being sent.



Plain Text	**C**	**R**	**Y**	**P**	**T**	**O**
Key	A	Y	S	Y	I	F
Cypher Text	D	Q	R	O	C	U

One-time-pad

- Share a “key” in advance. Secret and fully random.
- Use the “key” to encrypt/decrypt by adding the letters.
  - C = P+K mod 26
- Each letter gets a number: A=0, B=1 …
- Add the numbers (mod 26) to encrypt, subtract (mod 26) to decrypt
- One of the strongest forms of encryption.
- But… you have to pre-share keys that are at least as long as the plain text being sent.

Plain Text	**C**	**R**	**Y**	**P**	**T**	**O**
Key	A	Y	S	Y	I	F
Cypher Text	D	Q	R	O	C	U

Plain Text	**3**	**18**	**25**	**16**	**20**	**15**
Key	1	25	19	25	9	6
Add	4	43	44	41	29	21
Mod	4	17	18	15	3	21

One-time-pad

- Share a “key” in advance. Secret and fully random.
- Use the “key” to encrypt/decrypt by adding the letters.
  - C = P+K mod 26
- Each letter gets a number: A=0, B=1 …
- Add the numbers (mod 26) to encrypt, subtract (mod 26) to decrypt
- One of the strongest forms of encryption.
- But… you have to pre-share keys that are at least as long as the plain text being sent.

Cipher Text	**D**	**Q**	**R**	**O**	**C**	**U**
Key	A	Y	S	Y	I	F
Plain	C	R	Y	P	T	O

Cipher Text	**4**	**17**	**18**	**15**	**3**	**21**
Key	1	25	19	25	9	6
Subtract	3	-8	-1	-10	-6	15
Mod	3	18	25	16	20	15

One-time-pad

- One time pads are secure partially because they give plausible deniability
- The cypher text can be made to say anything of that length with the right key

Plain Text	**C**	**R**	**Y**	**P**	**T**	**O**
Key	A	Y	S	Y	I	F
Cypher Text	D	Q	R	O	C	U
Wrong Key	S	H	X	U	X	G
Fake Plain Text	**K**	**I**	**T**	**T**	**E**	**N**

One-time pad using Lorem ipsum as the key

Plaintext

margaret eleanor atwood cc o ont frsc poet novelist critic professor born november in ottawa on a varied and prolific writer margaret atwood is among the most celebrated authors in canadian history her writing is noted for its careful craftsmanship and precision of language which lend a sense of inevitability and a resonance to her words in her fiction atwood has explored the issues of our time capturing them in the satirical selfreflexive mode of the contemporary novel she has written novels nine shortstory collections books of poetry and volumes of nonfiction she has received two governor generals literary awards two booker prizes a scotiabank giller prize and numerous other honours and accolades she is a companion of the order of canada and a chevalier of the lordre des arts et des lettres of france

Key

Lorem ipsum dolor sit amet consectetur adipiscing elit sed do eiusmod tempor incididunt ut labore et dolore magna aliqua Lorem ipsum dolor sit amet consectetur adipiscing elit duis tristique Nulla facilisi etiam dignissim diam quis enim Non tellus orci ac auctor augue mauris augue neque Non odio euismod lacinia at quis risus sed vulputate Pharetra massa massa ultricies mi Odio ut sem nulla pharetra diam Nibh mauris cursus mattis molestie a iaculis at Integer eget aliquet nibh praesent tristique magna sit Scelerisque eu ultrices vitae auctor Tincidunt eget nullam non nisi est sit Faucibus scelerisque eleifend donec pretium vulputate sapien nec sagittis aliquam Tellus at urna condimentum mattis pellentesque id Vivamus arcu felis bibendum ut Velit dignissim sodales ut eu sem integer vitae Imperdiet proin fermentum leo vel orci porta Dignissim suspendisse in est ante in nibh mauris cursus mattis Morbi non arcu risus quis varius quam quisque Cursus mattis molestie a iaculis at erat Felis bibendum ut tristique et Imperdiet proin fermentum leo vel orci porta non pulvinar Sodales ut etiam sit amet nisl purus Eros donec ac odio tempor orci Nunc scelerisque viverra mauris in aliquam sem fringilla Cum sociis natoque penatibus et Vestibulum lorem sed risus ultricies tristique nulla aliquet Diam in arcu cursus euismod quis viverra Diam volutpat commodo sed egestas egestas Adipiscing tristique risus nec feugiat in fermentum posuere urna

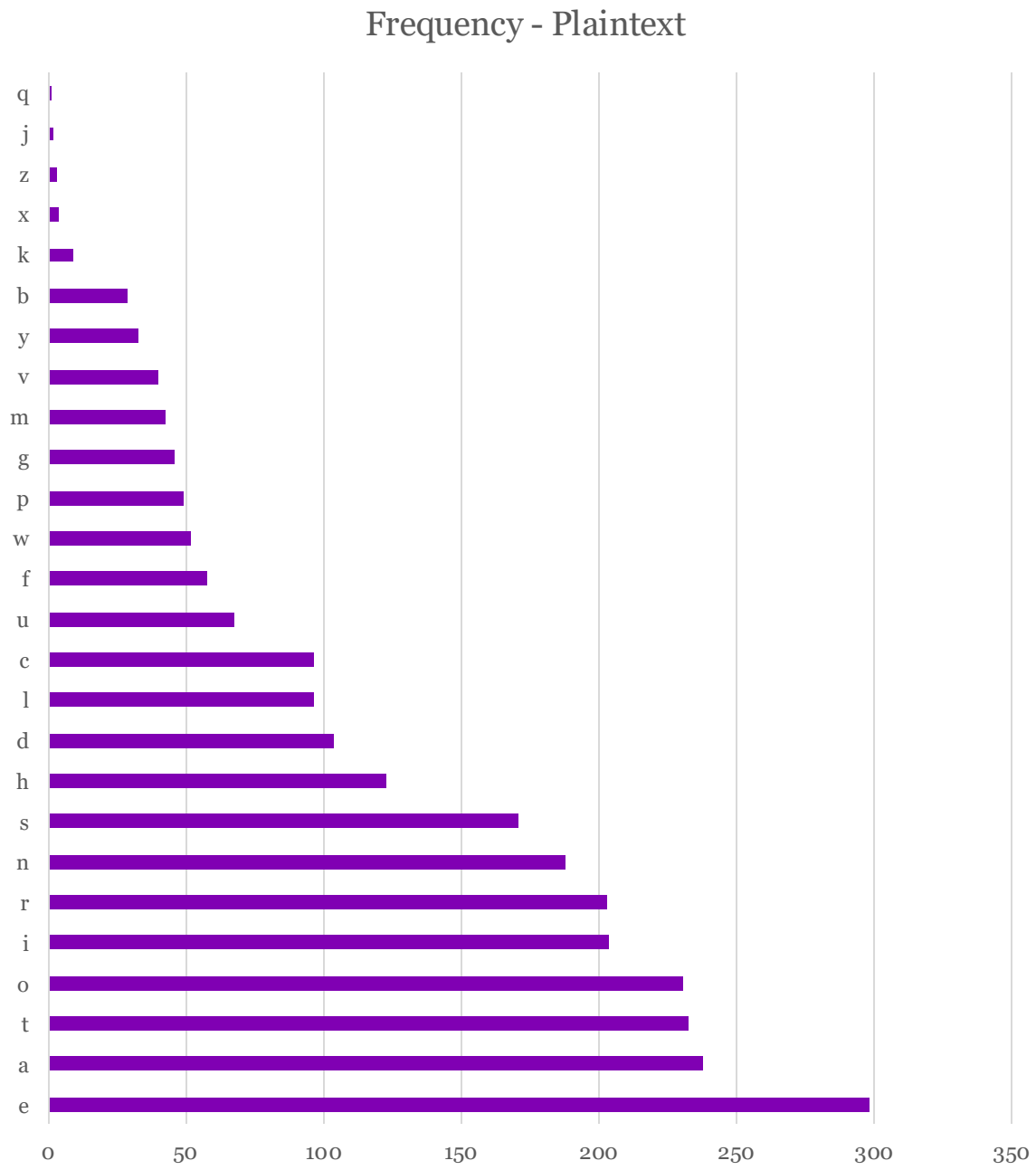
One-time pad using Lorem ipsum as the key

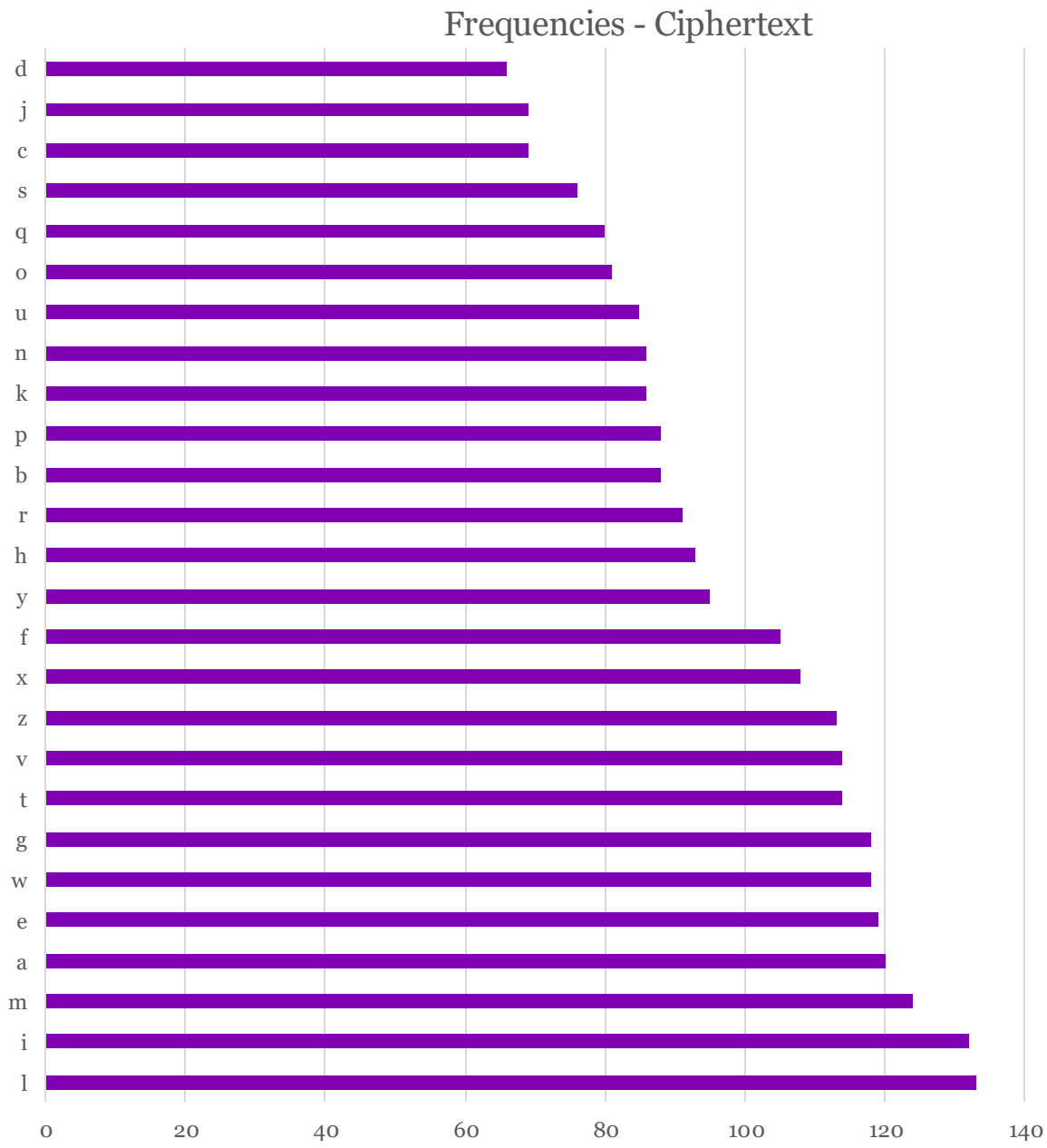
Plaintext

margaret eleanor atwood cc o ont frsc poet novelist critic professor born november in ottawa on a varied and prolific writer margaret atwood is among the most celebrated authors in canadian history her writing is noted for its careful craftsmanship and precision of language which lend a sense of inevitability and a resonance to her words in her fiction atwood has explored the issues of our time capturing them in the satirical selfreflexive mode of the contemporary novel she has written novels nine shortstory collections books of poetry and volumes of nonfiction she has received two governor generals literary awards two booker prizes a scotiabank giller prize and numerous other honours and accolades she is a companion of the order of canada and a chevalier of the lordre des arts et des lettres of france

Ciphertext

XOIKMZTLYXHOYCISBPOAHVECBFXHKWVJFEWV
DDWNQFZGCQMAGSUCJMMKAFEHVZCCMMZDMU
QQIGMUPLOOOMEVBHRLBUTDORVFINEHCTPFDE
DOPJYFDHHCFVQLAYSGIHUWQQLXVYCEEZPBWFI
HZLZZLLHKSGRLATVXCWGICJHJRYZTBAVKBANA
WMJSWJABEFIRQVOTUVNNFFANGWSTJSBURZEEI
MKHBFFFGHKGAAVEZIWNFIAHQMIAGRCIQBIPQL
MPLWIVGNVDAKUMWFRVUYLGLHMQZGXLIGLTY
FZGMZOZALOOADZSSYIICWTMHLTMWVAIYLGJAH
LETMTJAGXNIIQOTTRUJUFHYJILKLZUUDEEEYZW
RZPBAOMQOLEQZEPWCHVGXQVSIEXCGOGMBML
XUITDGZTXWRAHOVTKGQDYWTOXGSLWKQESWP
VKLYIRWVIZDJWHTGZBKYENXXHZLFMFQNQIAY
MIXBBHDSETNGERKWQZWWLEHLOPGZOIJYGRPV
RTKBCXICEZDEJDURFXYDSSHSYDKLTOYLALGGTX
IFNAOIALRMKIZAZPIDXNGFICZOKOMBVEHQBBXZ
EEAWUOOOETLWHWSPMFTGGCJEVLJVJFFBWOIF
YWSQKSOIEENQXMWAZZLTBHZUSBZWTAJRUEOI
KUKXMWXPMFEIZXIZAHFJZMCGV


Frequency - Plaintext
q
j
z
x
k
b
y
v
m
g
p
w
f
u
c
l
d
h
s
n
r
i
o
t
a
e
0
50
100
150
200
250
300
350


Frequencies - Ciphertext
d
j
c
s
q
o
u
n
k
p
b
r
h
y
f
x
z
v
t
g
w
e
a
m
i
l
0
20
40
60
80
100
120
140

Challenges in early crypto:

1. Sharing keys

2. Preventing frequency analysis

Security model of what a "good" cipher is

- **Perfect Security –** Given any ciphertext, all possible plaintexts of that length are equally likely
- **Concrete Security –** Adversary needs to do X work to break the cipher
- **Indistinguishability** - The adversary is not able to distinguish between two messages *M1* and *M2* of the same length
- **Random Oracle** - Ciphertext looks random in that there is no efficient way to distinguish it from a random function.

Think-pair-share

- For each of the security models on the right, think of an example where that type would be appropriate

- Prefect Security
- Concrete Security
- Indistinguishability
- Random Oracle

Two common solution approaches

Stream ciphers

- Encryption rule is dependent on a plaintext symbol's position in the stream of plaintext symbols.

Block ciphers

- Encrypt several plaintext symbols at once in a block.

Vigenère Cipher – Early Stream Cipher

- Uses a repeating key with a different length than the alphabet
- C = P+K mod 26
- Strong cipher (before computers)
- Still some patterns though in long texts so possible to break

Blaise de Vigenère
By Thomas de Leu - Woodcut Photograph.

```
 Plain  tobeornottobethatisthequestion
   Key  securitysecuritysecuritysecuri
Cipher  MCCICIACMMCCIMOAMQKMOIGOIKMQCA
```

Double Transposition Cipher – Simple Block Cipher

- Put the plaintext in an n x m array, pad if necessary.
- The key is the transposition of the columns and rows
- Moving the letters around in the cipher text makes frequency analysis less useful, but all the original letters are still present….

- "attack at dawn"

A	T	T	A
C	K	A	T
D	A	W	N

- Transpose the rows (1,2,3) -> (3,2,1)

D	A	W	N
C	K	A	T
A	T	T	A

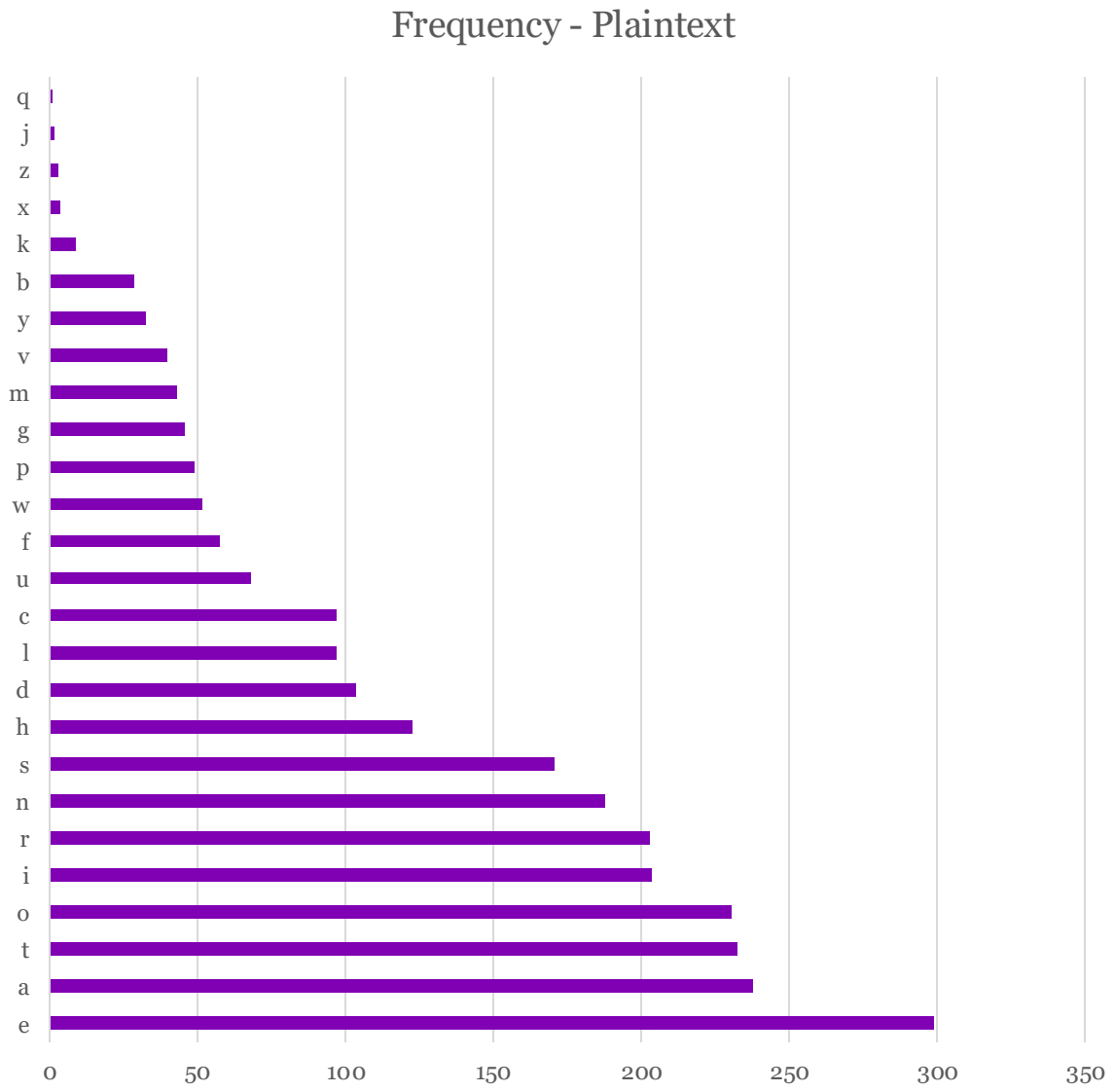
- Transpose the columns (1,2,3,4)->(4,2,1,3)

N	A	D	W
T	K	C	A
A	T	A	T

- Cipher: nadwtkcaatat

Double Transposition does not substitute letters

- Because the letters are not substituted, the frequency analysis will be the same before and after encryption
- The double transposition cipher instead scrabbles the letter order
- A modern computer should be able to re-construct the message by looking at the most probably word combination for the letters



Playfair Cipher – Early Block Cipher

- Use a key to create a grid of letters (omit j so there are 25 letters) similar to the earlier monoalphabetic substitution example:

```
abcdefghijklmnopqrstuvwxyz
SECURITYABDFGHJKLMNOPQVWXZ
```

- Convert the message into pairs of letters where x is inserted between repeated letters
- "Block" is the pair of characters

Key: Playfair Example

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

Plain text: Hello World

```
He lx lo Wo rl dx
```

Playfair Cipher – Early Block Cipher

Assume one wants to encrypt the digram OR. There are five general cases:

1)

```
* * * * *
* O Y R Z
* * * * *
* * * * *
* * * * *
```

Hence, OR → YZ

2)

```
* * O * *
* * B * *
* * * * *
* * R * *
* * Y * *
```

Hence, OR → BY

3)

```
Z * * O *
* * * * *
* * * * *
R * * X *
* * * * *
```

Hence, OR → ZX

4)

```
* * * * *
* * * * *
* O R W *
* * * * *
* * * * *
```

Hence, OR → RW

5)

```
* * * * *
* * R * *
* * O * *
* * I * *
* * * * *
```

Hence, OR → IO

Key: Playfair Example

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

Plain text: Hello World

HE LX LO WO RL DX

Diagram HE -> DM

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

Stream vs Block

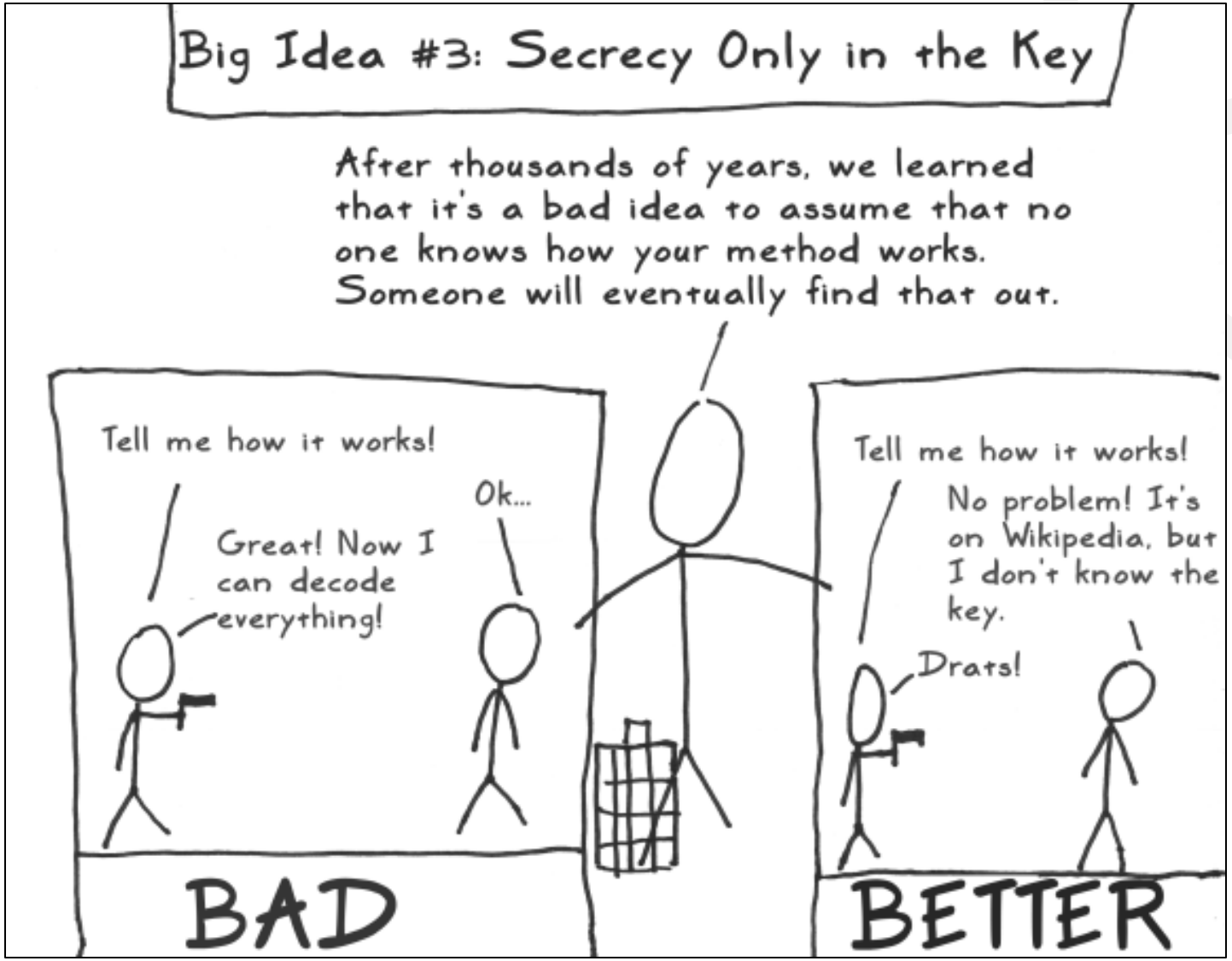
Stream Ciphers

- Pros
  - Speed of transformation, each character can be encrypted/decrypted as it comes in
  - Low error propagation, a transcription error on one character will not impact the other characters
- Cons
  - Low diffusion, one character in plaintext results in one character of ciphertext
  - Susceptible to malicious insertions and modifications

Block Ciphers

- Pros
  - High diffusion, information from the plaintext is spread across several ciphertext characters
  - Immunity to insertion, inserting one character will cause issues in deciphering
- Cons
  - Slow to encrypt, the entire block must be encrypted/decrypted at once
  - Padding, message must be a certain length and sometimes irrelevant text must be added
  - Error propagation, an error in one character will impact all other characters in the block

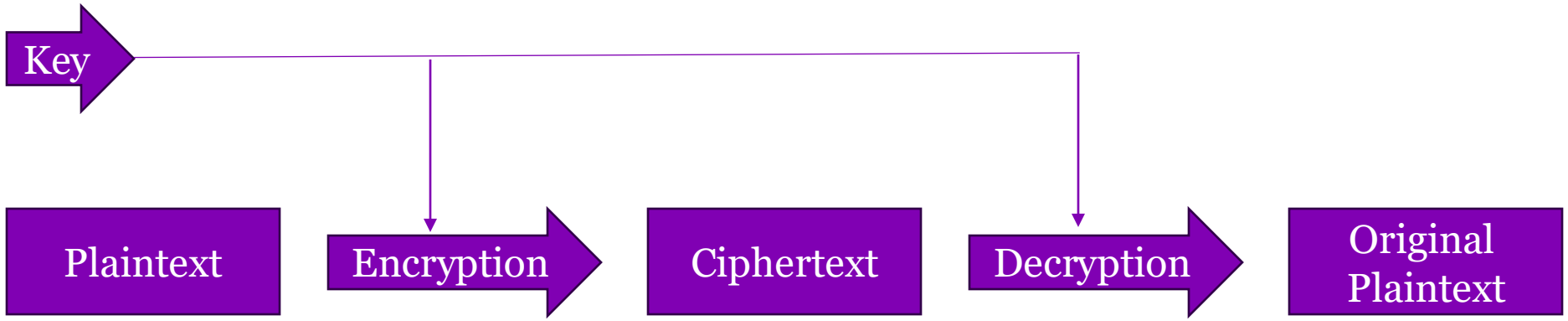
Assume the attacker knows how the crypto is done



https://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

Symmetric ciphers

- The prior examples are all symmetric ciphers where the same key is used for encryption and decryption
- Sharing the key can be problematic



Asymmetric ciphers

- Different keys are used to encrypt and decrypt
- Public/private key encryption is one of the more famous asymmetric ciphers

SP-Networks (Substitution and Permutation Circuits)

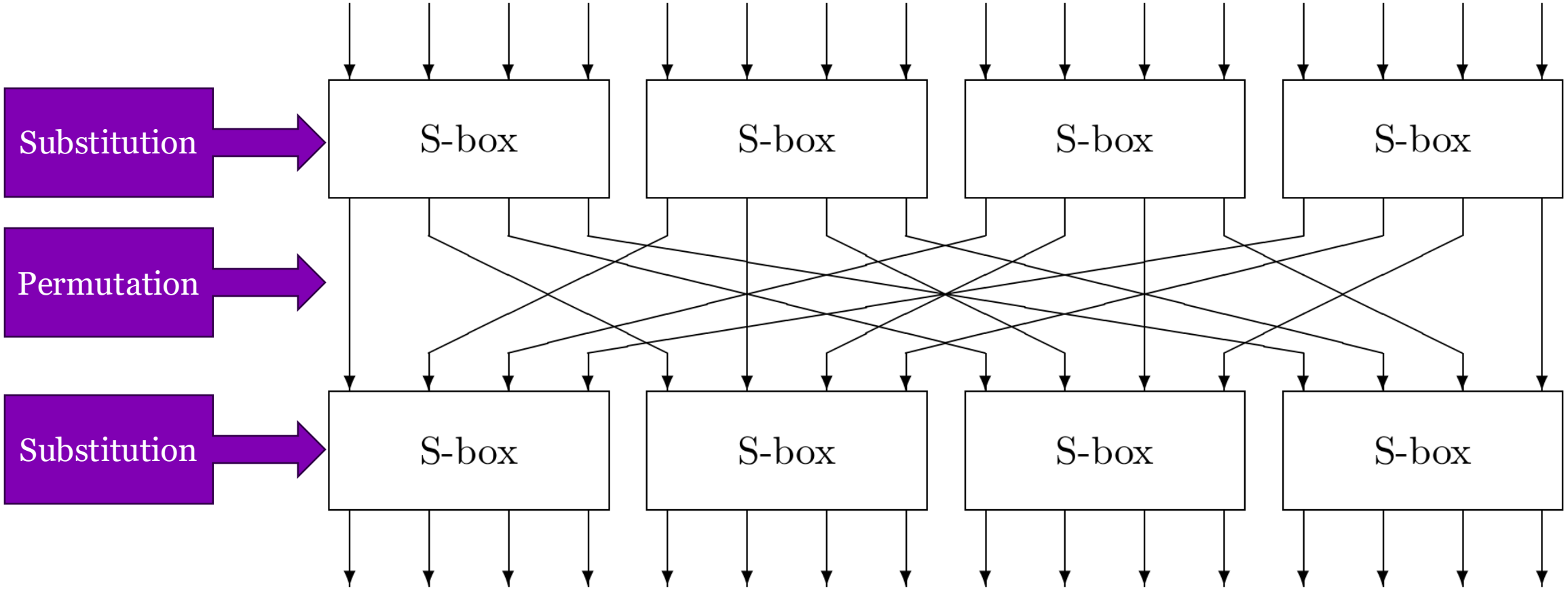
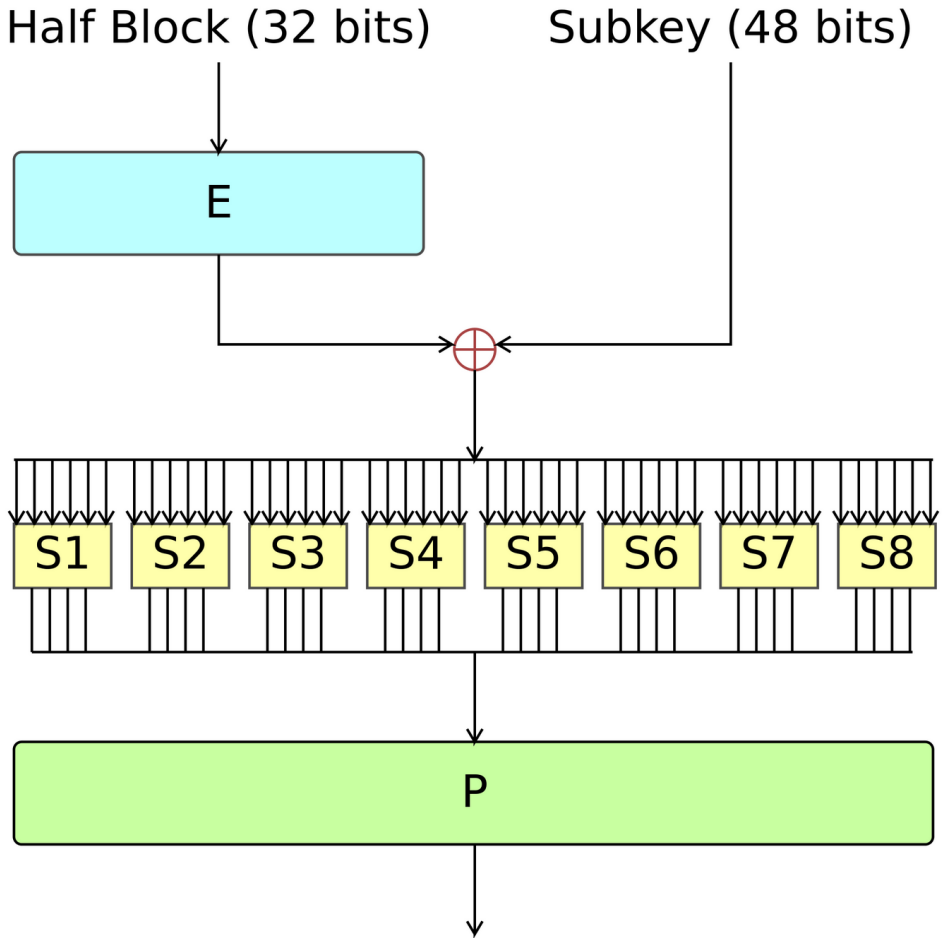


Figure 5.10: – a simple 16-bit SP-network block cipher

Security Engineering, v3 by Ross Anderson, Ch 5.4

Data Encryption Standard (DES)

- Symnetric-key algorithm using 56 bit keys and a block cipher
- Developed in 1970s at IBM
- Approved by NSA (after key length shortened) leading to quick adoption
- January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (Wikipedia)



By Hellisp - File:Data Encryption Standard InfoBox Diagram.png, CC0

QUESTIONS