

# ECE458/ECE750T27: Computer Security

## Cryptography

Dr. Kami Vania  
Electrical and Computer Engineering  
[kami.vania@uwaterloo.ca](mailto:kami.vania@uwaterloo.ca)



UNIVERSITY OF  
**WATERLOO**

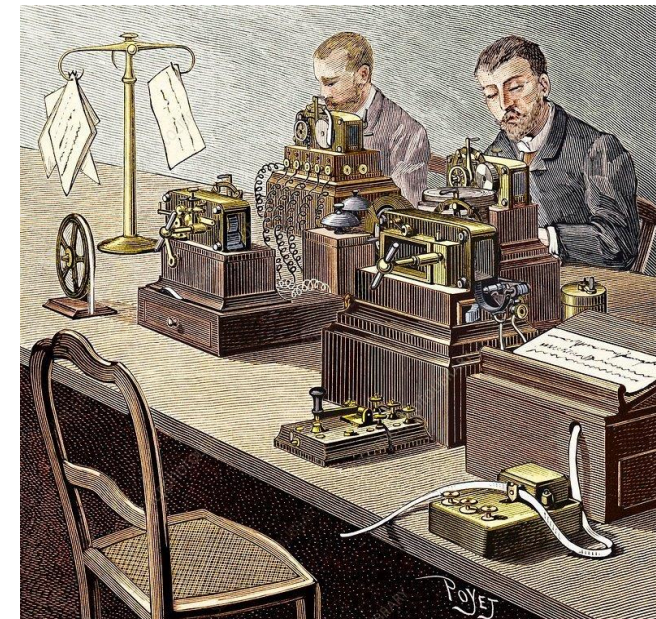
FACULTY OF  
ENGINEERING



# A BIT OF HISTORY FOR CONTEXT

# Telegraphs

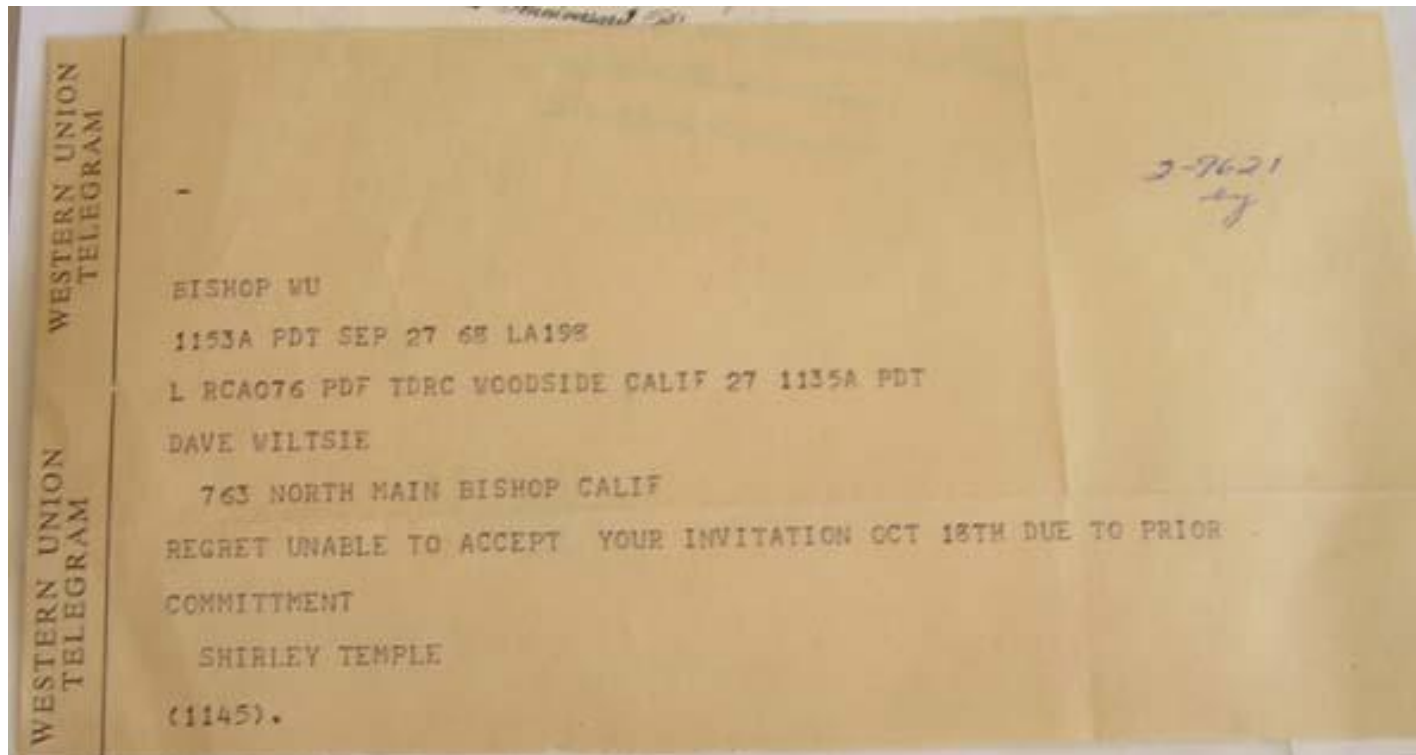
- Messages used to be sent via telegraph
  - 1844: First telegraph message sent
  - 1866: Telegraph wires between US and Europe
- The operator pushes down on the button creating a "beep" as long as they press



# Telegraphs

- No way to send a letter through a telegraph, so Morse Code was invented

Telegraph sent to my grandfather in 1965 from an actress apologizing for missing his party.



## International Morse Code

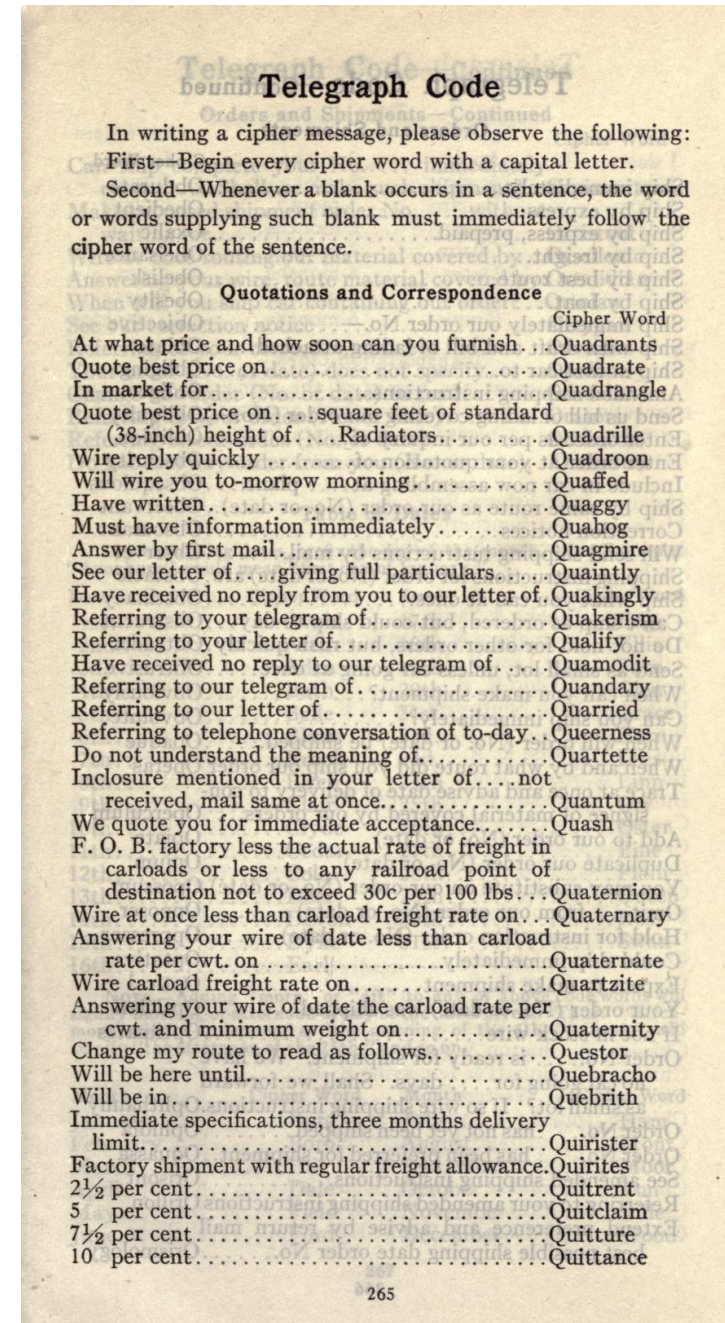
1. The length of a dot is one unit.
2. A dash is three units.
3. The space between parts of the same letter is one unit.
4. The space between letters is three units.
5. The space between words is seven units.

|   |         |
|---|---------|
| 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 | — — • •   |
|   |           |
| 1 | • — — — — |
| 2 | • • — — — |
| 3 | • • • — — |
| 4 | • • • • — |
| 5 | • • • • • |
| 6 | — • • • • |
| 7 | — — • • • |
| 8 | — — — • • |
| 9 | — — — — • |
| 0 | — — — — — |

# Telegraph Codebooks

- Each letter was expensive to send
- Security was poor since anyone with physical access to the wire could listen
- Codebooks were used to convert common phrases to shorter words, different companies/groups used different codebooks
- Uncommon words, phrases or numbers still sent directly



# Codebooks also used alongside encryption


- Idea: before encrypting switch out important unique words for codes
  - "Toronto" -> "Wichita"
- The codebook is now much shorter so easier to remember and store
- If the encryption is broken, all is not lost because key parts of messages still missing


## How Codebreakers Helped Secure U.S. Victory in the Battle of Midway

Advanced intelligence helped the Allies turn the tables on Japan in this crucial World War II naval battle.

BY: SARAH PRUITT

UPDATED: APRIL 15, 2024 | ORIGINAL: NOVEMBER 6, 2019

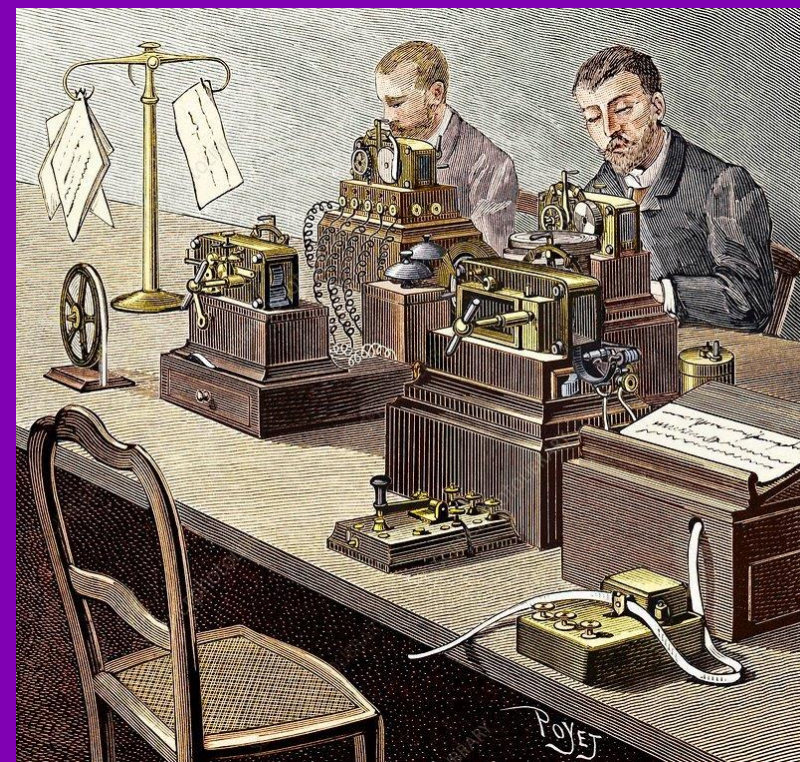
 [copy page link](#)

 [PRINT PAGE](#)

- US Navy codebreakers decrypted that Japan planned to attack "AF"
- US guessed that AF was Midway base. To test, the base intentionally transmitted unencrypted that they were low on water
- A Japanese transmission was then intercepted stating that "AF" was low on water

**The point: keep the realities of technology in mind as we discuss older cryptography.**

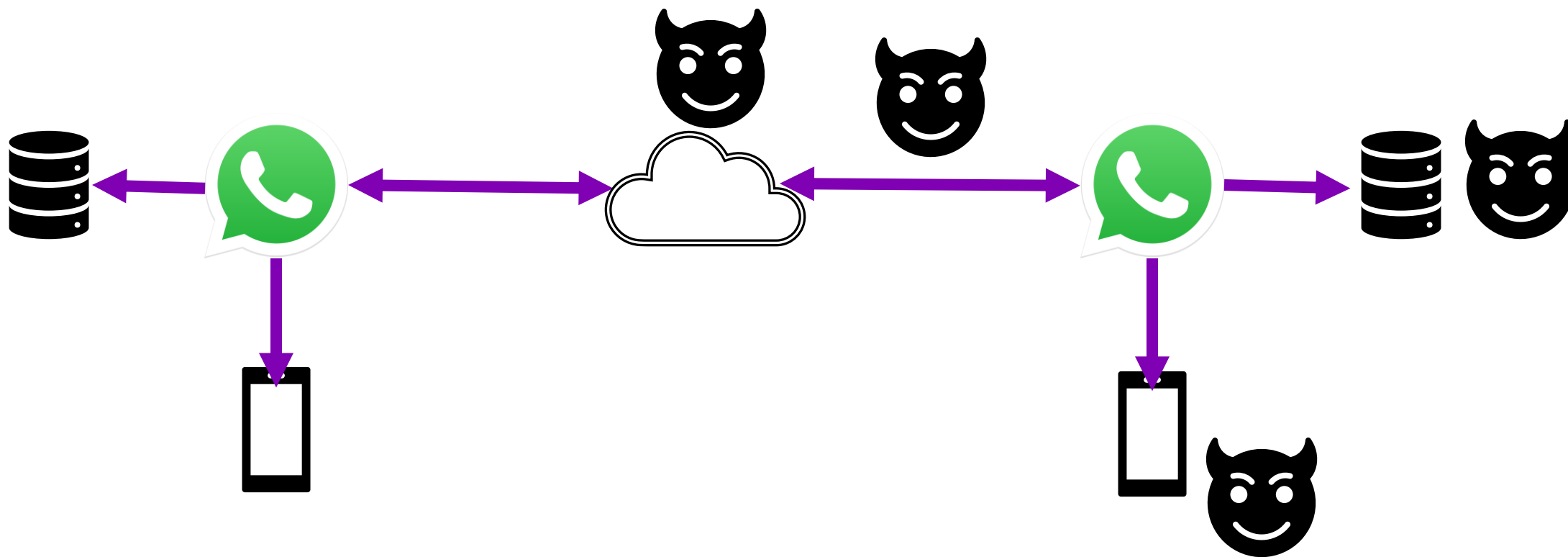
**A cryptographic algorithm needs to work reliably and quickly for the computer (human or machine) that does the encryption and decryption.**



# Last time we talked....

- Caesar Cipher – letter substitution using offset
- Monoalphabetic Substitution – letter substitution where letter order is more randomized
- One-time-pad – plaintext is added to a key of equal length
- Vigenère Cipher – stream cipher using a repeating key
- Double transposition cipher – plaintext is put in a block and the rows and columns are transposed
- Playfair cipher – a matrix is constructed from a key and plaintext is encrypted in letter pairs
- Security models: Perfect Security, Concrete Security, Indistinguishability, Random Oracle

**Data exists in different places, and the approaches to protect it differ with the place it is.**



# 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:  $P = D(K, C)$
- **Ciphertext**, **Plaintext**, **Encryption rule**, **Decryption rule**, **Key**

# PLAYFAIR CIPHER

# 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 |

# 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  
SECURITYABDFGHJKLMNPOQVWXZ

- 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 |

# Playfair Cipher – Early Block Cipher

Prepare the plaintext for encryption.

- Insert x between repeated letters.
- Replace any 'j' with 'i'.
- If an odd number of letters, add an x to the end.
- Convert the message into pairs of 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

- **Rectangle:** pick from same row but opposite corner
- **Column:** pick letter one row down, wrapping if necessary.
- **Row:** pick letters one step to right, wrapping if necessary.

|   |   |   |   |   |
|---|---|---|---|---|
| Z | * | * | O | * |
| * | * | * | * | * |
| * | * | * | * | * |
| R | * | * | X | * |
| * | * | * | * | * |

Hence, OR → ZX

|   |   |   |   |   |
|---|---|---|---|---|
| * | * | O | * | * |
| * | * | B | * | * |
| * | * | * | * | * |
| * | * | R | * | * |
| * | * | Y | * | * |

|   |   |   |   |   |
|---|---|---|---|---|
| * | * | * | * | * |
| * | * | R | * | * |
| * | * | O | * | * |
| * | * | I | * | * |
| * | * | * | * | * |

|   |   |   |   |   |
|---|---|---|---|---|
| * | * | * | * | * |
| * | O | Y | R | Z |
| * | * | * | * | * |
| * | * | * | * | * |
| * | * | * | * | * |

Hence, OR → YZ

|   |   |   |   |   |
|---|---|---|---|---|
| * | * | * | * | * |
| * | * | * | * | * |
| * | O | R | W | * |
| * | * | * | * | * |
| * | * | * | * | * |

Hence, OR → RW

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 (rule 3)

|   |   |   |   |   |
|---|---|---|---|---|
| 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 |

# Playfair of Margaret Atwood text with “Playfair Example” key

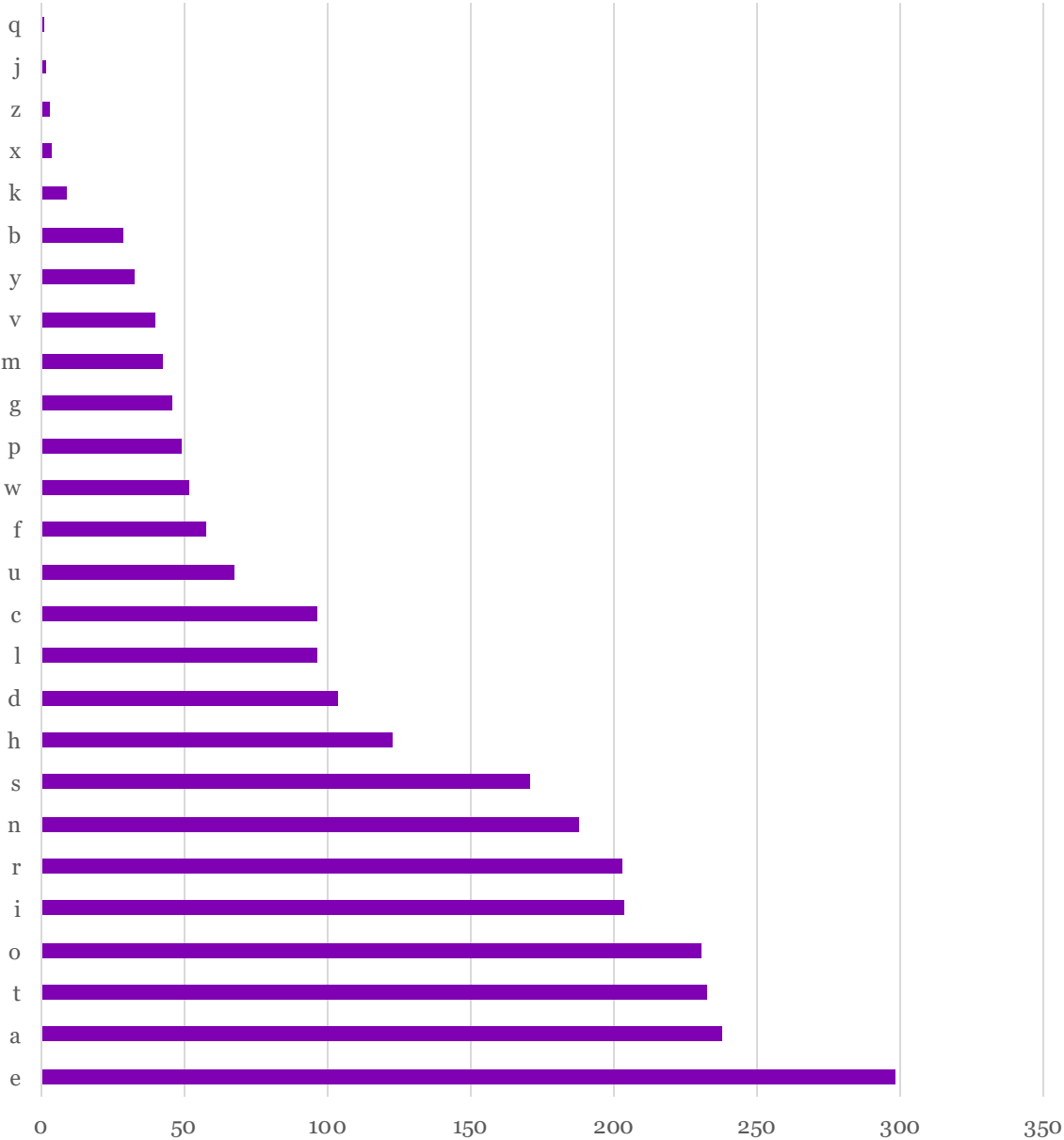
## Plaintext

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

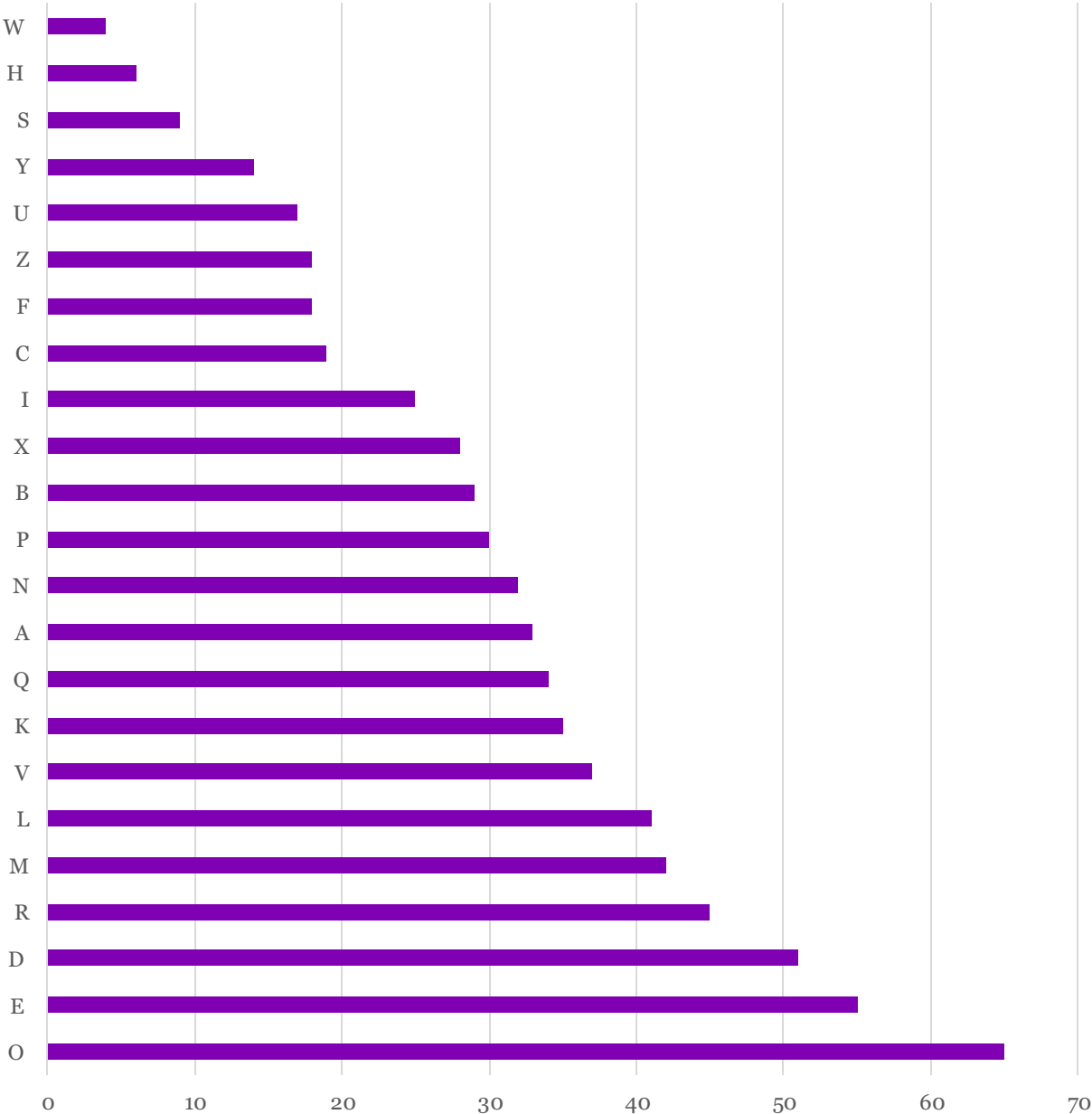
## Ciphertext

EFXCLEIV RADEOQE LUZQEVO, GRD, N QOZ, PMNB, LVDU, KVARAMKU, BERPBB, LENAMQMKQI (CNEQ 18 ROQADIHXE 1939 RK KVVVPVY, QO). E ALERXO EOC LINAMPRB UXBPXE, EFXCLEIV PVVQVO MK FEQOB WDM ESKZ DRARCIPVDO LVZBNEK MU NLOEOEPS CMKVKXL. DMX UERPBQC MK OQVIH ANE BPN HLEMALR NCYPZKEFOKBML YOC LIRDMKEKO QP ALOCWYDX, VBMD B AROC F OROOM SA RKDABPPDRPBPF YOC L EMOQOLODR VK DMX UNEHO. RK DMM LRBPBQO, PVVQVO DFO MIYANEXB VDM MKNZMO SA NVI URIR, DYLUVERQC ZBXI RK ZBM OPVRERBYA, OMAP-EXPAXMETX IVOD VP ZDM DNKUXIAKELXL OQADF. NDM DFQ ZERWIVIQ 14 ROQADFN, KROR ZSNEZ-KVKXL DNYRARBUEKOK, 16 DKQNK QP LVDUIF, YOC 10 AVR LIXK QL SQO-PMBUEKO. KDM DFN MRDXRADB VVQ DQADCUNE DORELFN PRVIELXL YVLEHO, UZK DQEONXE LIMTMO, F ODNBPDPLOQ BRPARI LERVM, LOC OZR XENVK QZBXE DSOQLCO FOC LDDNAYODQ. MZSX RO F DNIFLOEKO QP ZDM NEODE NL HLOEOY ELOO E DBDAYARXE NP ZDM A'NECEX ODO FIUO MV BMO ARWIUIMO SA LMLODR.

Frequency - Plaintext



Frequencies - Ciphertext



# 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



# We discussed:

## Substitution

- Vigenère Cipher

```

Plain  tobeornottobethatisthequestion
Key    securitysecuritysecuritysecuri
Cipher MCCICIACMMCCIMOAMQKMOIGOIKMQCA
  
```

- Characters are substituted for other characters

## Permutation

- Double Transposition Cipher

|         |   |         |   |         |
|---------|---|---------|---|---------|
| A T T A |   | D A W N |   | N A D W |
| C K A T | → | C K A T | → | T K C A |
| D A W N |   | A T T A |   | A T A T |

- Character positions are moved around

**We discussed what these approaches look like when done correctly**

**Now lets look at two examples where substitution and permutation are done poorly**

# XOR plaintext with the key - Stream Cipher

- Letters in files are all ASCII
- One (bad) idea is to XOR a file against a repeating key (Vigenère Cipher).
- Very easy for computers to do
- Approach is bad for many reasons:
  - All the frequency and pattern problems of a Vigenère Cipher
  - Most common character in an English text file is the space
  - XOR is symmetric, if I XOR the cyphertext with the space character, the output will be characters of the password which happen at 8-bit boundaries

## XOR Truth Table

| P | K | C =<br>$P \oplus K$ |
|---|---|---------------------|
| F | F | F                   |
| F | T | T                   |
| T | F | T                   |
| T | T | F                   |

## Reverse an XOR

| C | K | P =<br>$C \oplus K$ |
|---|---|---------------------|
| F | F | F                   |
| T | T | F                   |
| T | F | T                   |
| F | T | T                   |

# XOR of Margaret Atwood text with “security” key

## Plaintext

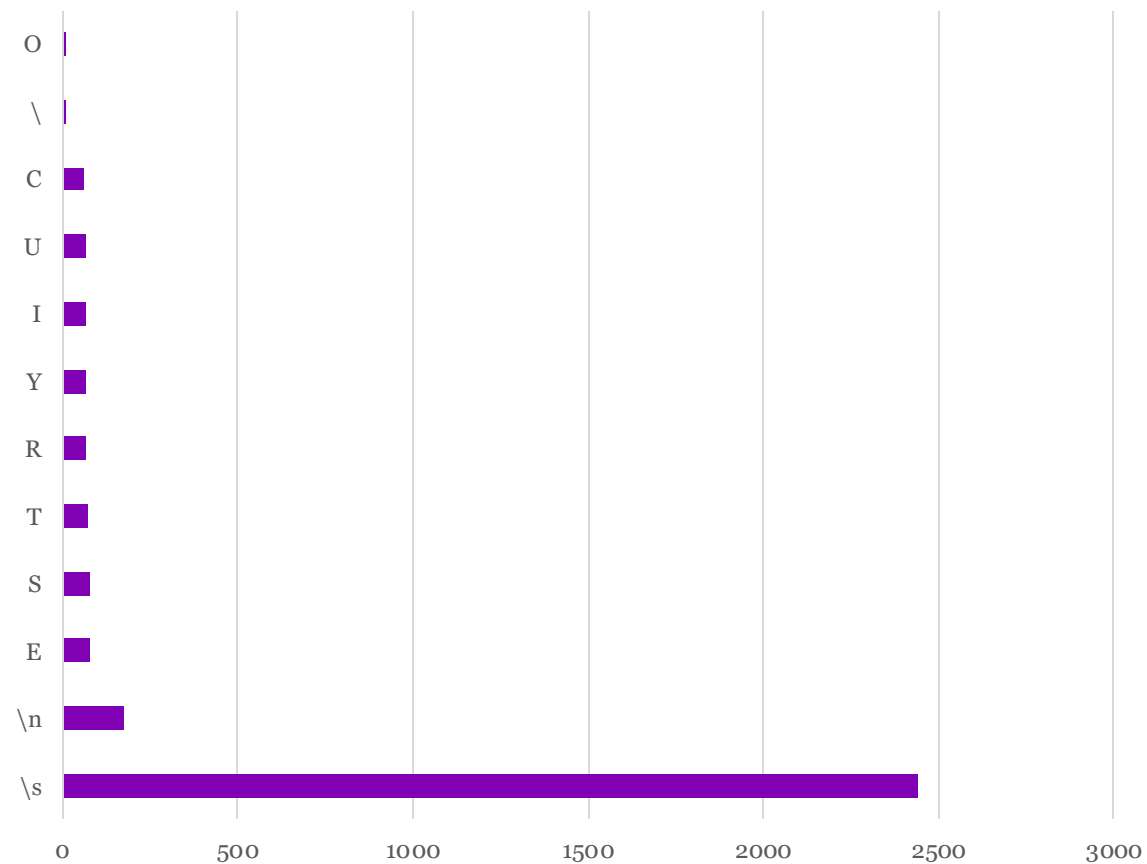
margaret eleanor atwood cc o ont frsc poet novelist critic professor born november in ottawa on a varied and prolific writer margaret atwood is among the most celebrated authors in canadian history her writing is noted for its careful craftsmanship and precision of language which lend a sense of inevitability 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 (newlines removed)

S S US YRT OU \_E XY \_E \_E  
 UZ ERM IE@@\C I ^I ZKC R U  
 Y S US E S U E I C I I  
 S E KC T T E Y U Y Y I  
 E U T US T UI U T R SC  
 R Y U KC I E IC E I T C E R  
 S ET S I S R XY \_ T U T C  
 Y GT C T THGE \_E T \_ C  
 XYBSC S U OU YBUC C I H KC T  
 C U Y S E C IC T I ^I Y  
 C E US R I U U Y KC T E  
 U I S R C I { SC R Y UN U  
 Y R Y U U T G

# XOR with “security” key

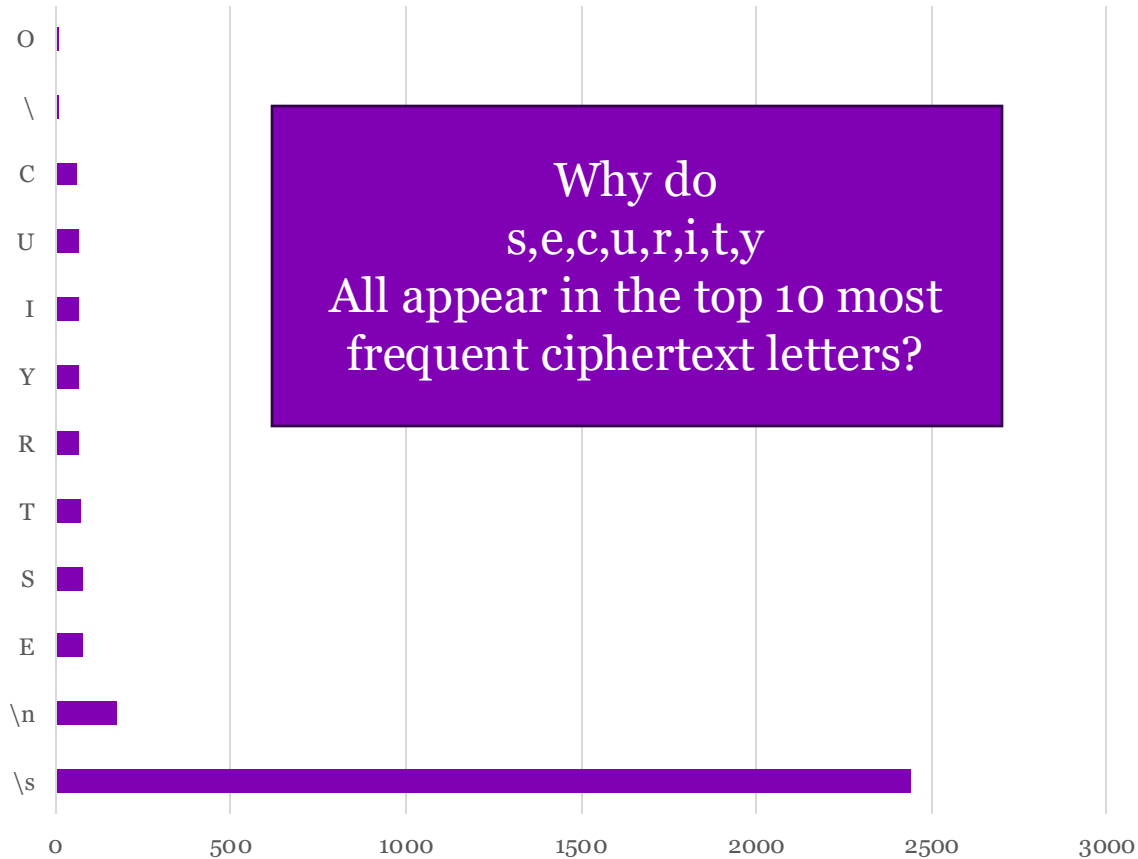
Ciphertext Character Frequency (top 12)



- The distribution to the left is weird
- Discuss with your neighbor what is weird about it.

# XOR with “security” key

Ciphertext Character Frequency (top 12)



- Space is the most common character in ASCII, represented by a binary 32
- S and s in ASCII differ by the 32 bit position
- So if we XOR a space and an ASCII character, we will get the lower/upper case of that character back

|          |             |
|----------|-------------|
| 00100000 | Space       |
| 01010011 | S character |
| 01110011 | s character |

# Block cipher where no information is shared between blocks

- Double Transposition Cipher shown to the right
- OK-ish cipher if all the text fits in one block
- Most modern text is long and requires multiple blocks, if each block is computed independently, then repeated text becomes visible
- "attack at dawn"
 

|   |   |   |   |
|---|---|---|---|
| A | T | T | A |
| C | K | A | T |
| D | A | W | N |
- Transpose the rows  $(1,2,3) \rightarrow (3,2,1)$ 

|   |   |   |   |
|---|---|---|---|
| D | A | W | N |
| C | K | A | T |
| A | T | T | A |
- Transpose the columns  $(1,2,3,4) \rightarrow (4,2,1,3)$ 

|   |   |   |   |
|---|---|---|---|
| N | A | D | W |
| T | K | C | A |
| A | T | A | T |
- Cipher : nadwtkcaatat

# Plaintext broken across blocks, no information shared

- Plaintext: attack at dawn then break off attack at dawn

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A | T | T | A | T | H | E | N | A | T | T | A |
| C | K | A | T | B | R | E | A | C | K | A | T |
| D | A | W | N | K | O | F | F | D | A | W | N |

- Transpose the rows (1,2,3)  $\rightarrow$  (3,2,1)

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| D | A | W | N | K | O | F | F | D | A | W | N |
| C | K | A | T | B | R | E | A | C | K | A | T |
| A | T | T | A | T | H | E | N | A | T | T | A |

- Transpose the columns (1,2,3,4)  $\rightarrow$  (4,2,1,3)

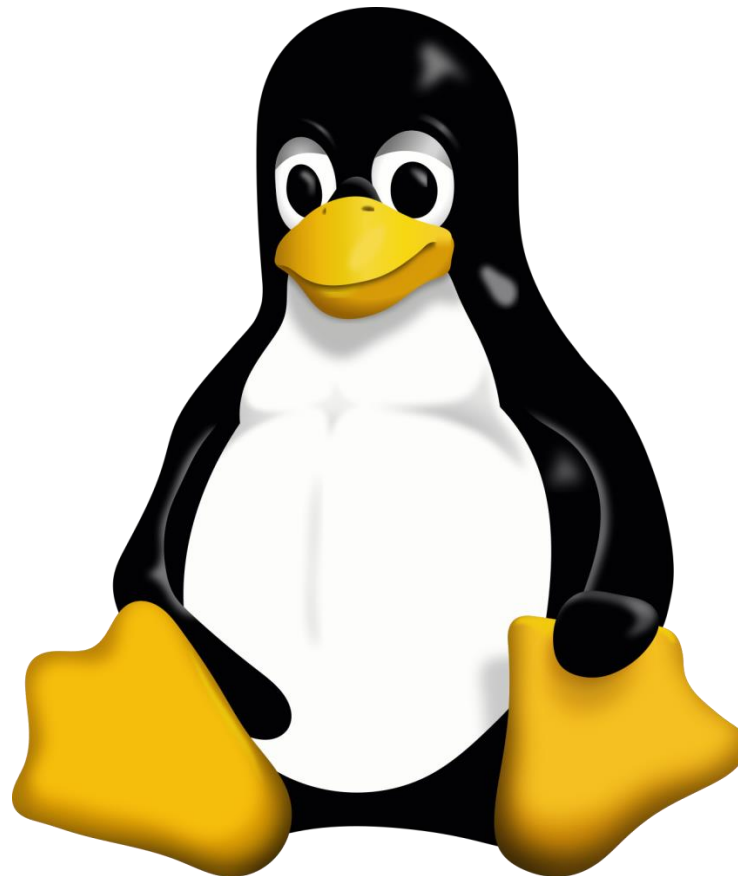
|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| N | A | D | W | F | O | K | F | N | A | D | W |
| T | K | C | A | A | R | B | E | T | K | C | A |
| A | T | A | T | N | H | T | E | A | T | A | T |

- Cipher: nadwtkcaatat fokfarbenhte nadwtkcaatat

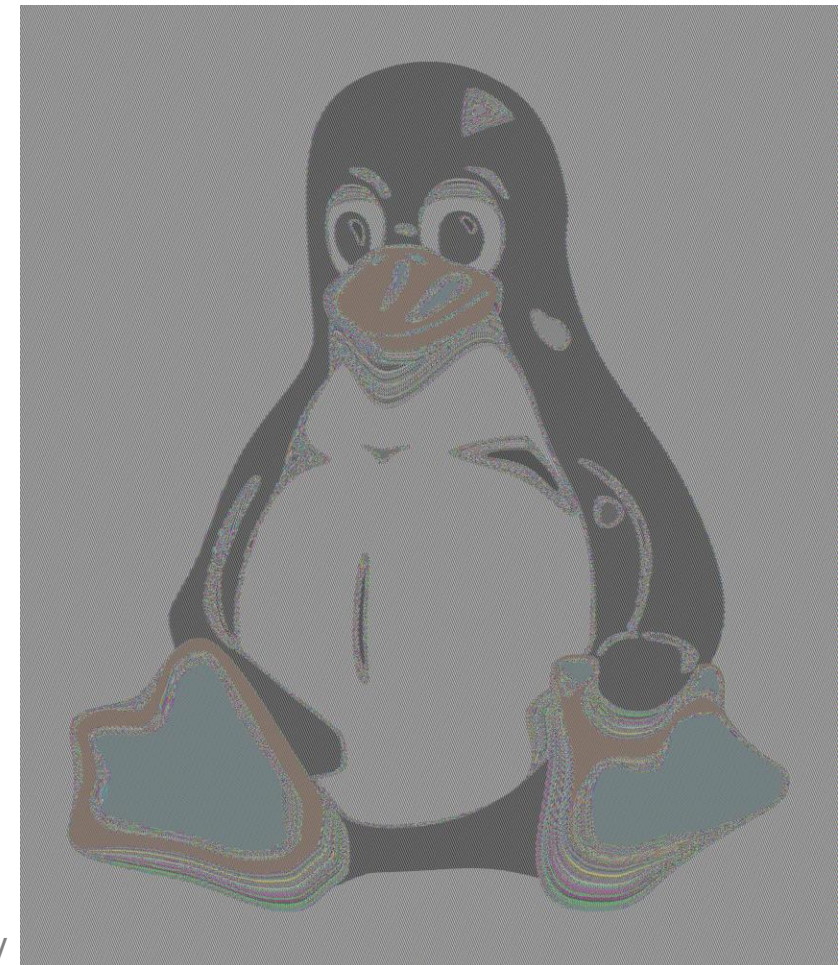
# ECB Penguin: what happens when block ciphers don't mix text between blocks

- Images are just binary text files so they can be encrypted
- Tux image has large blocks of solid color, scrambling the order of a block of nearly identical values does little
- Encrypted using AES-128 (Good crypto) using ECB (isolate blocks, bad idea)

Plaintext

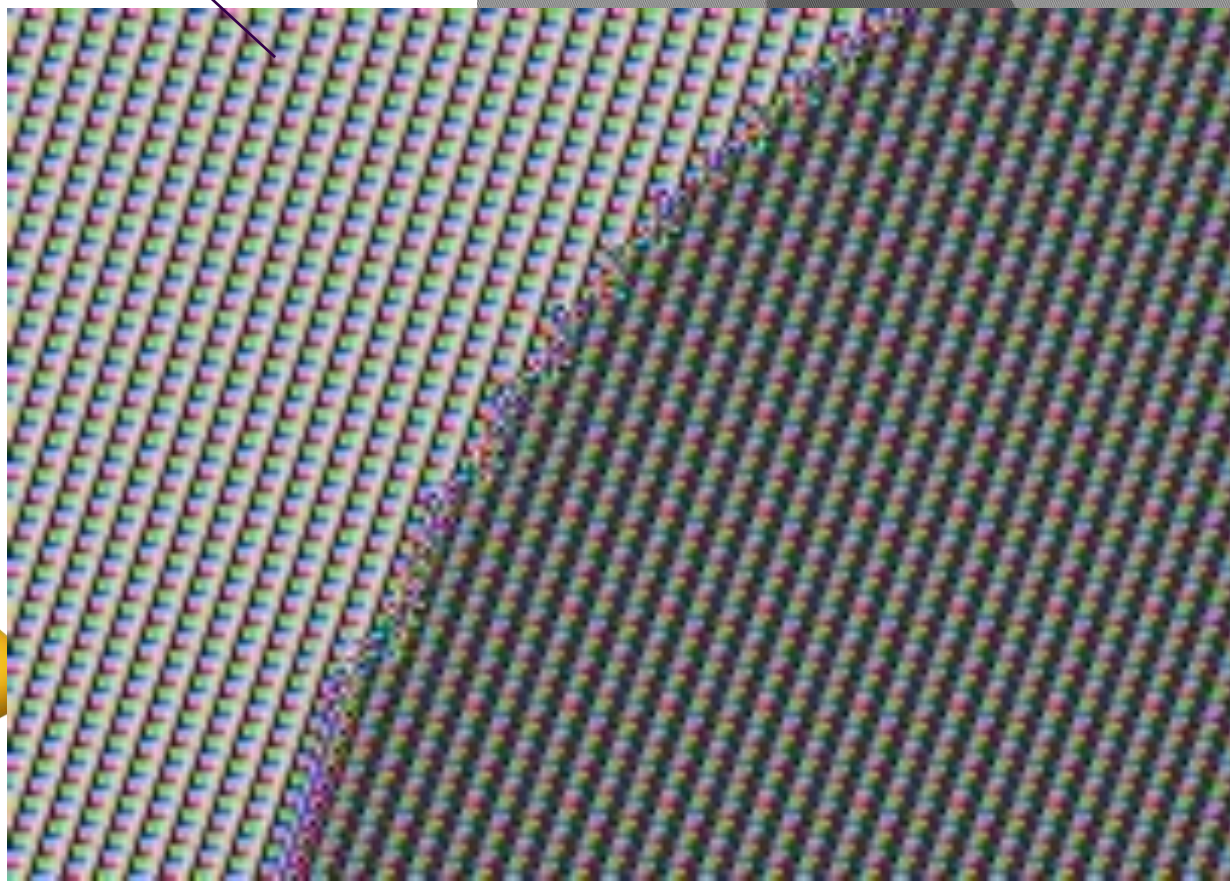
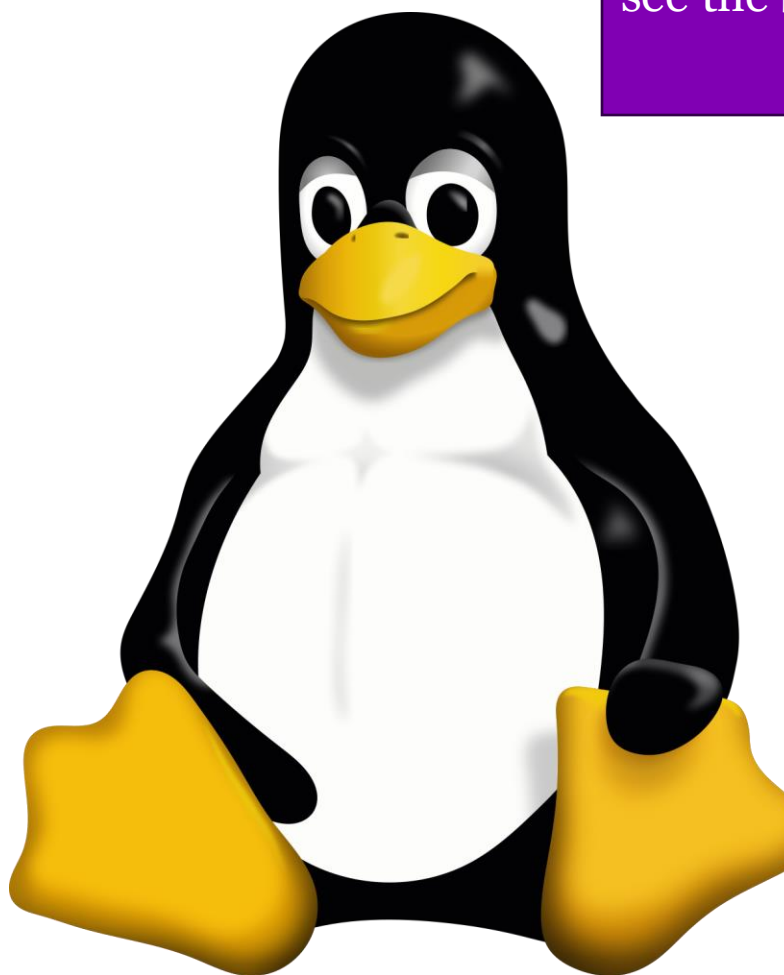


Ciphertext



# ECB Penguin: what happens with block ciphers that don't mix text between blocks

If we zoom in, you can see the block edges in the image



# Modern encryption is done on computers

- Historical encryption/decryption had to be done by hand, often with pencil and paper, so the old methods are designed in human-friendly structures
  - Humans also handle shorthand, missing words, and irrelevant information well
- Modern cryptography is done using computers, so general purpose crypto needs to be fast on standard CPU architectures
- For example: Playfair is designed to be visual, and easy for people.
- Computers are better at binary operations such as addition, xor, and shift. As well as clear rules like 'x' means null
- Computers complete many iterations of the same task easily

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 |

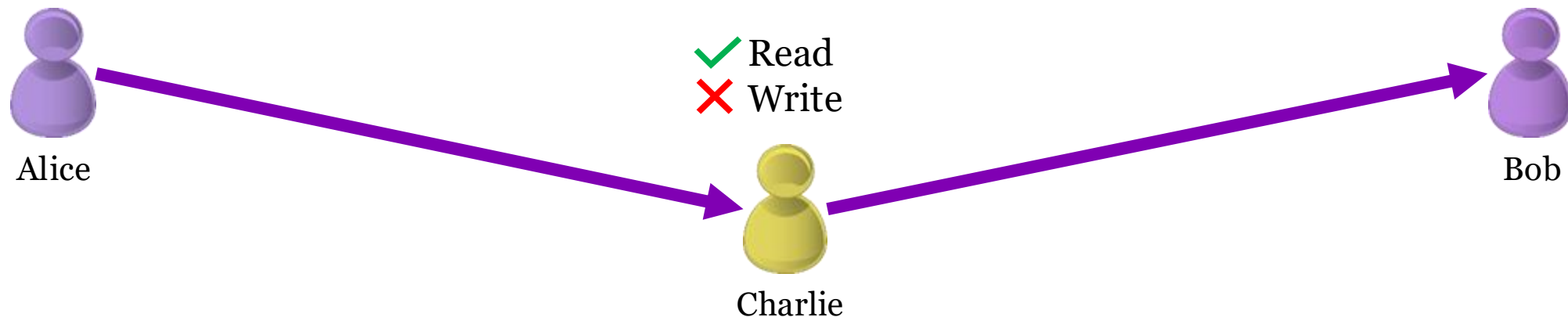
# Think-pair-share

- Things computers can do better than a human cryptographer
- Things computers do worse than a human cryptographer

# **HASH FUNCTIONS DEMONSTRATING INTEGRITY**

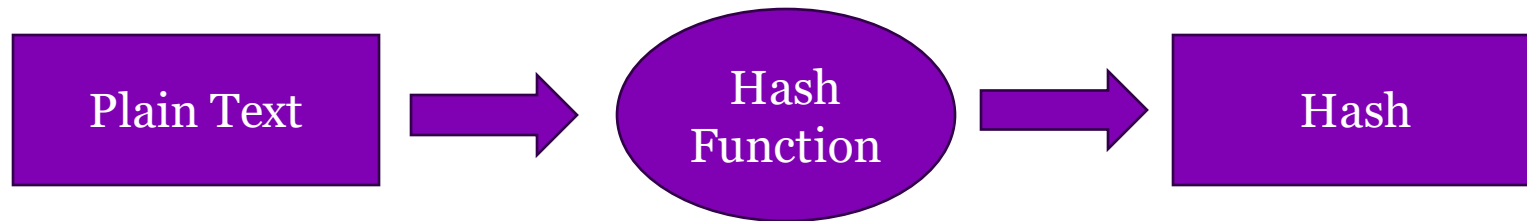
# Integrity and Authenticity are quite important...

- **Confidentiality** is the goal of most of the ciphers discussed thus far.
- **Integrity** and **Authenticity** can be more important in some situations.



# Hashing

- A hash is a one way function. So the same plaintext will always produce the same hash. But the hash cannot be used to produce the plaintext.



# AES-256 encryption of Margaret Atwood text with password "security"

## 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

U2FsdGVkX1/xq+nopPiEU7hz8Kg3es/c/mfqJIF5KXJxmzFmDfZOybu7kAP1Svb+Cagks2fnn7Vjad+TfCqjGAdMYLnmoHzMAoAI1qaU2UpgSGI+ERm5QslymtuiI+Be oL9yu5WZZbriPqsQhkiM3SqWEYrZBoaSlIOAYZgONbAsEgBtWEM2v2Pwfnw8CIG znhutBNeWpx6lBKqOfIKdp81fg8X885ZE7CPBB6bIJKk9ckfrgPUesK2X/4yyADs 1lhEi3qvKv98EHKFQyTomgzJPw9p5k7rw82PdM/zo6Dn7kLFiLtAI7OFqzNTl9xo R5qCkC6mRhsexpibaXbjgT9e2DVF+PXvzrWkwlmXuE3dVzfuIEtSiP1Os2NXa8d7d i9JJrUTpTOnNNsdLbRUsrOP2owyy6DCarjkUqKOhlmJ2XA8ClgSix4ycrBpF3IG vXOKR1P9tmERXPQ670BdCb5AkexEcQByQMSQXv5GoZ7kwCutwjaLOClAKWwSC6sQ q7Z86T88rhqE1d/E+L3rC84jQeTFs5lUmm7JoEX1+/Ulp5a5aznhsYbLmMd78mpD GdARBrKtVTbFHz3vP8nZncwXSVblGMS1c4Hkiq7yuokf/Y4rCq3GKehtoapWAJ61 QtlAovlOMjev1C4/83IgESfeNYc9kHLuNo+Dso8QE01mz1q1ymbSHYBUcEoXmofy d3kSUoSS1clEMsvEOa2FKple7s2DJUC3YDWA vBokfgjuYc4SC+mnEeGmVRHaLxgX QoofyiSMUJtnJ6exXvabBdQU8V3SSWDvrzKWw7LLVHEEwcMDiEiA7LZStro9P85D v7AMfUCcoXsPbkqqXVex33Z7wPrrtR7k+Zp+lo2hEraeqxUHElBbgP778n/t7W 1ov2RoorBonuZefmM+duGZhMXAxSEEm5kHUjlnOTWK1UcjlYyzLIWCHEOosoG8D+ XzM6ecbDWAZ9Hx1uDf539yQx8XETRpk8B649BYnHR3uC5IEkeMiZ+xiP3Osmh1m NxfJvsd77/arFWF5/YV7c8L2bbq51S/bI6TrgbfHU6wsuBwbvkhI2cRfg/S3QHAv Y5JedZzBS3tQHUylwYJazY8RJLcAvUbrT/+CeS3e2jpRaLMnUeB/vsaDwPI3NznV iecAaI4G6QoF2Runyi41Kfp4diLRKpNJnLtU1xFO8cl=

# Hash of Margaret Atwood text - sha256

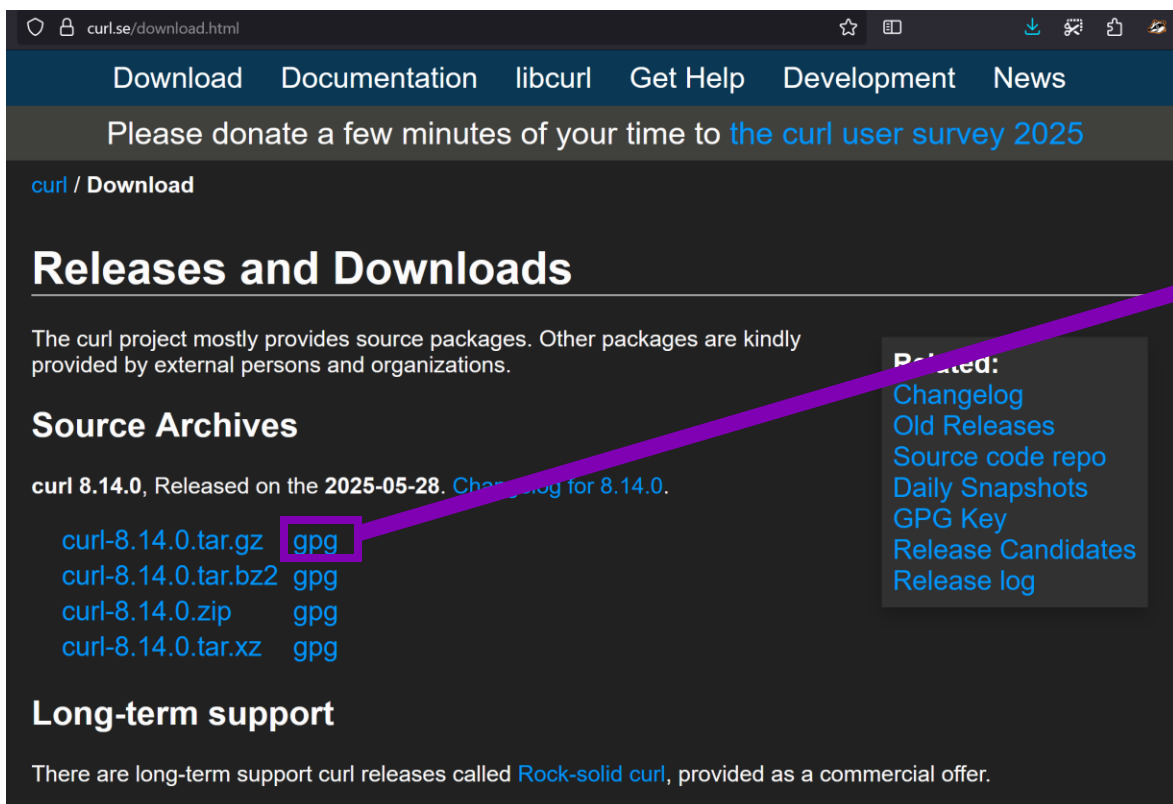
## Plaintext

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

## Hash (Ciphertext)

b9e1af100b214e17ead5d2be2aeod578d61c931f7b4d  
a165df4fd9ed45e4240c

# Verify correct download



The screenshot shows the curl website's download page. A purple arrow points from the 'gpg' link in the 'Source Archives' section to the PGP signature block on the right.

curl.se/download.html

Download Documentation libcurl Get Help Development News

Please donate a few minutes of your time to [the curl user survey 2025](#)

curl / Download

## Releases and Downloads

The curl project mostly provides source packages. Other packages are kindly provided by external persons and organizations.

### Source Archives

curl 8.14.0, Released on the 2025-05-28. [Changelog for 8.14.0.](#)

|                                     |                     |
|-------------------------------------|---------------------|
| <a href="#">curl-8.14.0.tar.gz</a>  | <a href="#">gpg</a> |
| <a href="#">curl-8.14.0.tar.bz2</a> | <a href="#">gpg</a> |
| <a href="#">curl-8.14.0.zip</a>     | <a href="#">gpg</a> |
| <a href="#">curl-8.14.0.tar.xz</a>  | <a href="#">gpg</a> |

### Long-term support

There are long-term support curl releases called [Rock-solid curl](#), provided as a commercial offer.

**Related:**

- [Changelog](#)
- [Old Releases](#)
- [Source code repo](#)
- [Daily Snapshots](#)
- [GPG Key](#)
- [Release Candidates](#)
- [Release log](#)

-----BEGIN PGP SIGNATURE-----

iQEzBAABCgAdFiEEJ+3q8i86vOtQ25oSXMkI/bceEsIFAmg2omI  
ACgkQXMkI/bce  
EsKJ4wf+NPfi0hF8jqZNYx9kHdRhEHuWuleksTetYlKWV6bN1z4  
wl+sJXbDwxFo8  
kkcPXOmSrX5f2kdQ0KYdHOnx7qX2zQiTvLzMWLUeMyLEghFclwY  
qKo2ykYHqDDzm  
eYujaifD/B3Ru8gNyGDhB+uXLyjRcmiw9/AA3qzGBNx6mqN4V8J  
DQ6/TdI4Ydky6  
+Um55zCXQVwqYJCJvz/2TZVw3jwzxWNRKSH12055NGqp/JqjC86  
KglauH4Ge1aT+  
Z5O5xNEBYkdNZVapiXHtYQvKMTURF+woAjVmgoIKkgmq1wD2Mxu  
ihGeGwwp84gvF  
SaQSkzSZ+xs0H9ZoTkWh5YLfvt2nzA==  
=IlNc

-----END PGP SIGNATURE-----

# Hashing files to check for changes

```
kami@porcupine:~/git/ece458-course/content/lectures/cryptography$ ls
06-CryptographyIntroduction.pdf  crypto-intro-handout.pdf  _index.md
kami@porcupine:~/git/ece458-course/content/lectures/cryptography$ sha256sum 06-CryptographyIntroduction.pdf
e007743db7c6c5729610684b070ea758cd0b71d0773396960ae18da72d8ba15f 06-CryptographyIntroduction.pdf
kami@porcupine:~/git/ece458-course/content/lectures/cryptography$ sha256sum 06-CryptographyIntroduction.pdf
e007743db7c6c5729610684b070ea758cd0b71d0773396960ae18da72d8ba15f 06-CryptographyIntroduction.pdf
kami@porcupine:~/git/ece458-course/content/lectures/cryptography$ sha256sum _index.md
ebe492500458067d7008428acd48d3c8791aac3abad495514f88361bfff0427a _index.md
```

Kami then edits `_index.md`

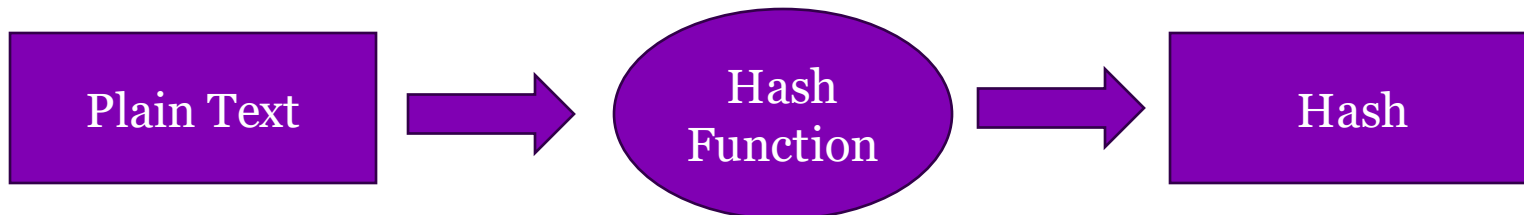
```
kami@porcupine:~/git/ece458-course/content/lectures/cryptography$ sha256sum _index.md
4adbc9eb515847fcedee8530b3bc182eb78781565bb89d959b2b8ce1a770a8ac _index.md
```

# Hashing passwords

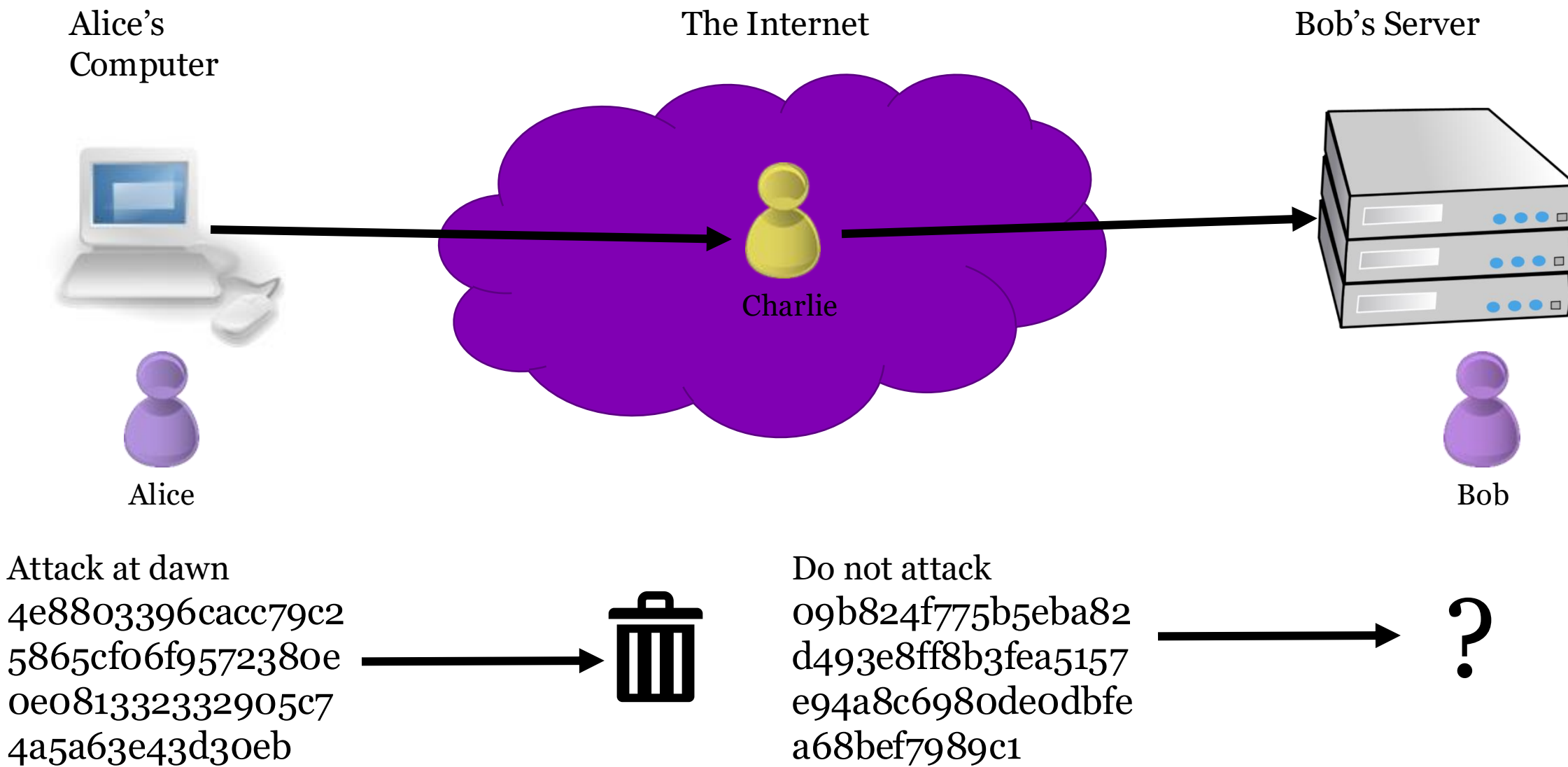
A row from /etc/shadow

aychedee:\$6\$vb1tLY1qiY\$M.1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cuMFzTRANcNKFKR4RmAQV4k4rqQQCkaJT6wXqjUkFcA/qNxLyqW.U/:15405:0:99999:7:::

- There are two ways to protect a password on a server:
  - You can encrypt the password and keep the key in a *really really* safe place
  - You can hash the password. Hashing does not require a secret key so there is no secret key to lose
- A hash is a one way function. So the same password will always produce the same hash. But the hash cannot be used to produce the password.



# Normal hash cannot prove integrity or authenticity



# Historical Bank Example

- Banks were heavy users of telegraphs and worried about modification of communications by telegraph clerks
- They used simple mathematical computations of important values and included the "test key" in the message
- In modern terms they computed a hash or a checksum
- Algorithm and table only known to bank employees, so the "test key" provided integrity and authenticity

*'To Lombard Bank, London. Please pay from our account with you no. 1234567890 the sum of £1000 to John Smith of 456 Chesterton Road, who has an account with HSBC Bank Cambridge no. 301234 4567890123, and notify him that this was for "wedding present from Doreen Smith". From First Cowboy Bank of Santa Barbara, CA, USA. Charges to be paid by us.'*

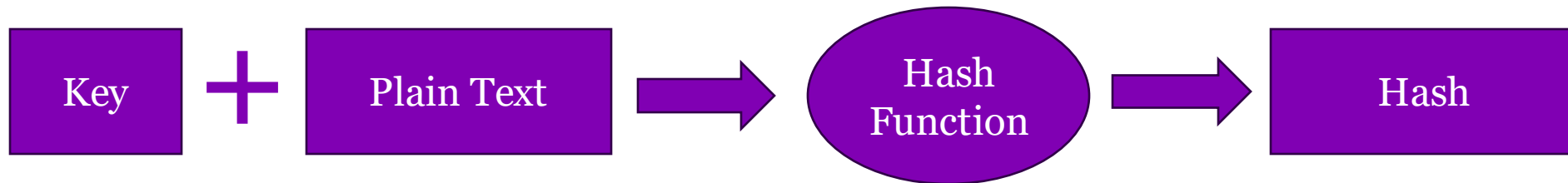
|             | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
|-------------|----|----|----|----|----|----|----|----|----|----|
| x 1000      | 14 | 22 | 40 | 87 | 69 | 93 | 71 | 35 | 06 | 58 |
| x 10,000    | 73 | 38 | 15 | 46 | 91 | 82 | 00 | 29 | 64 | 57 |
| x 100,000   | 95 | 70 | 09 | 54 | 82 | 63 | 21 | 47 | 36 | 18 |
| x 1,000,000 | 53 | 77 | 66 | 29 | 40 | 12 | 31 | 05 | 87 | 94 |

*Figure 5.8 – a simple test key system*

Now in order to authenticate a transaction for £376,514 we might add together 53 (no millions), 54 (300,000), 29 (70,000) and 71 (6,000) ignoring the less significant digits. This gives us a test key of 207.

# Hashing + key

- A simple trick is to concatenate a key onto the plaintext.
- Only someone with the key could have produced that hash.



# Hash-based message authentication code (HMAC)

- There are many algorithms that can create an HMAC using a message and a key
- Overly simple algorithm:
  - Divide 128-bit key into two 64 bit keys ( $k_1$ ,  $k_2$ )
  - Treat  $k_1$  like it was a salt and hash the message +  $k_1$  producing a 64bit cipher  $C_1$
  - XOR  $C_1$  and  $k_2$ 
    - $C_2 = C_1 \oplus k_2$
- Send the unencrypted message and  $C_2$
- The recipient has  $k_1$ ,  $k_2$  already, so they can verify the message by doing the same computation.
- An attacker without the  $k_1$ ,  $k_2$  cannot brute force  $C_2$

# HMAC of Margaret Atwood text sha-1 with key "security"

## 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

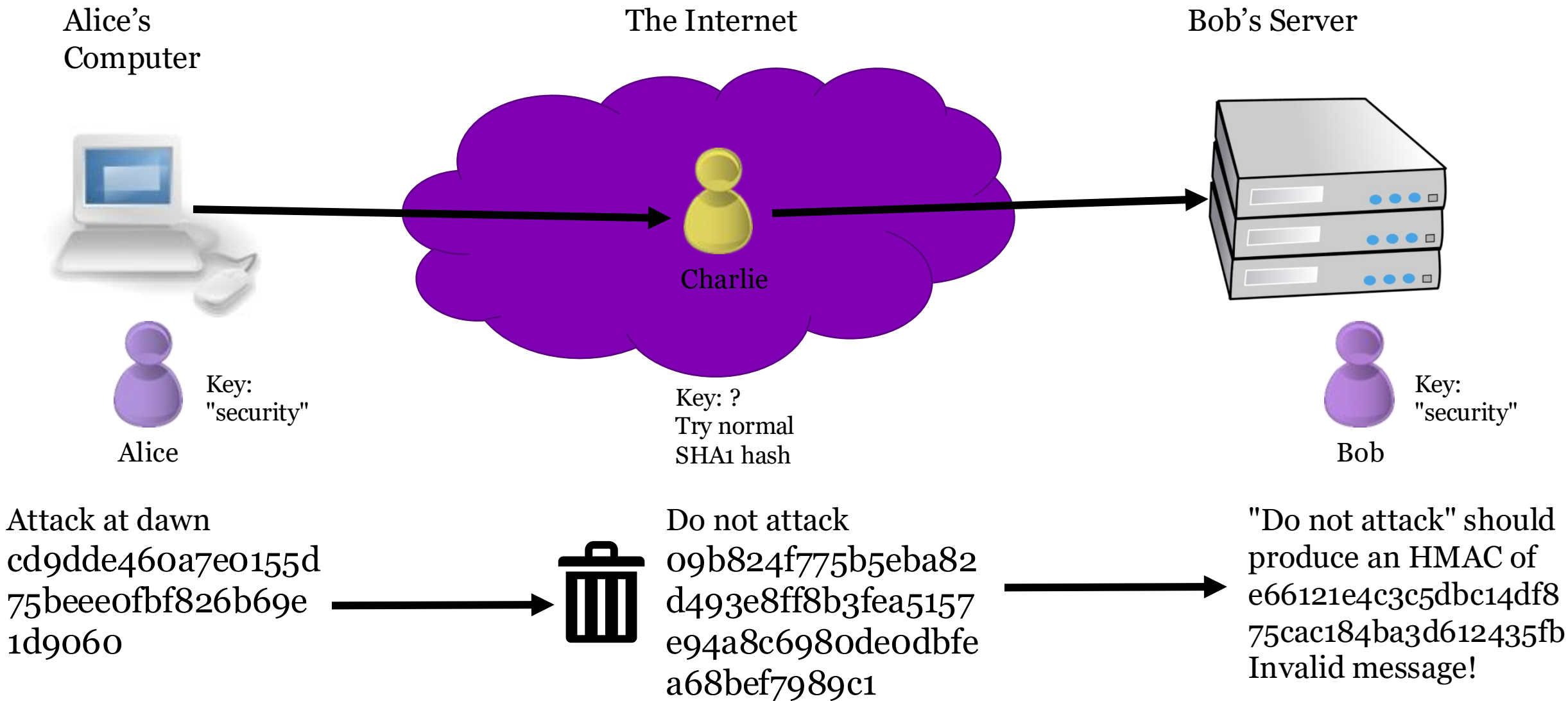
## Hash (Ciphertext)

e27020defe9c3116220e2dc8fa9e30a088365484

When using HMAC, both the message  
AND the HMAC hash are sent.

```
cat margaret-atwood-para1.txt | openssl dgst -sha1 -hmac "security"
```

# HMAC using SHA1 and key "security"



# Hashing for passwords vs messages

## Password Hashes

- Password hash stays on a (hopefully) secure computer with strong access restrictions
  - Password file itself has integrity
- We want to prove that the user **knows** the correct password aka plaintext
- Hashes + salt allow proof that the given password matches the old password without having to store a password
  - Password confidentiality
  - Authenticity proven by providing correct password

## Message Hashes

- Messages are sent between devices, they can be modified in transit
- Hash itself can be modified if it is sent between devices
- We want to prove that the **message is not modified** and sent by an **authorized person**
- Hashes + keys allow proof of integrity and authenticity

# Hashes can provide integrity, depending on what you want

- Password storage and later comparison – normal one-way hash
- Verify that a downloaded file was not modified in transit – normal one-way hash (assuming secure access to posted expected hash value)
- Verify that a message from a known communicating partner has not been changed – HMAC hash

# 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



**Idea: try combining substitution and permutation in the same cipher algorithm**

# SP-Networks (Substitution and Permutation Circuits)

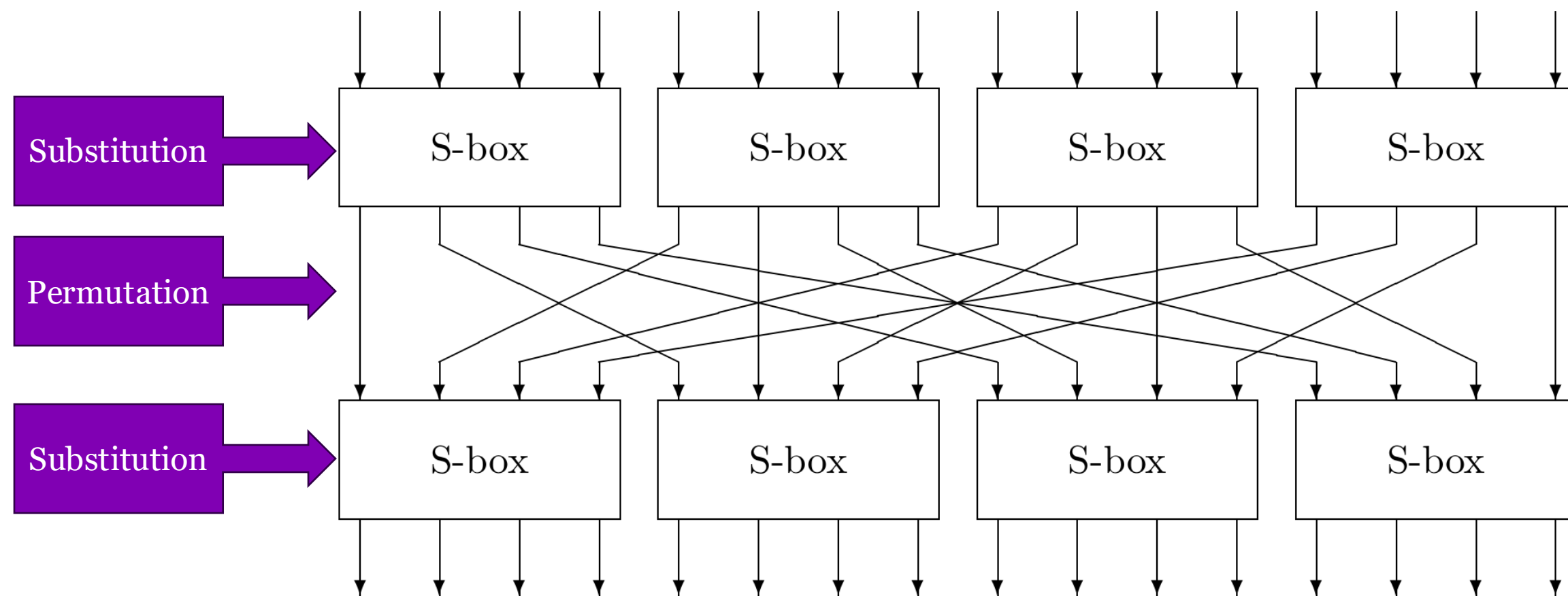


Figure 5.10: – a simple 16-bit SP-network block cipher

# Information Dispersion in SP-Networks

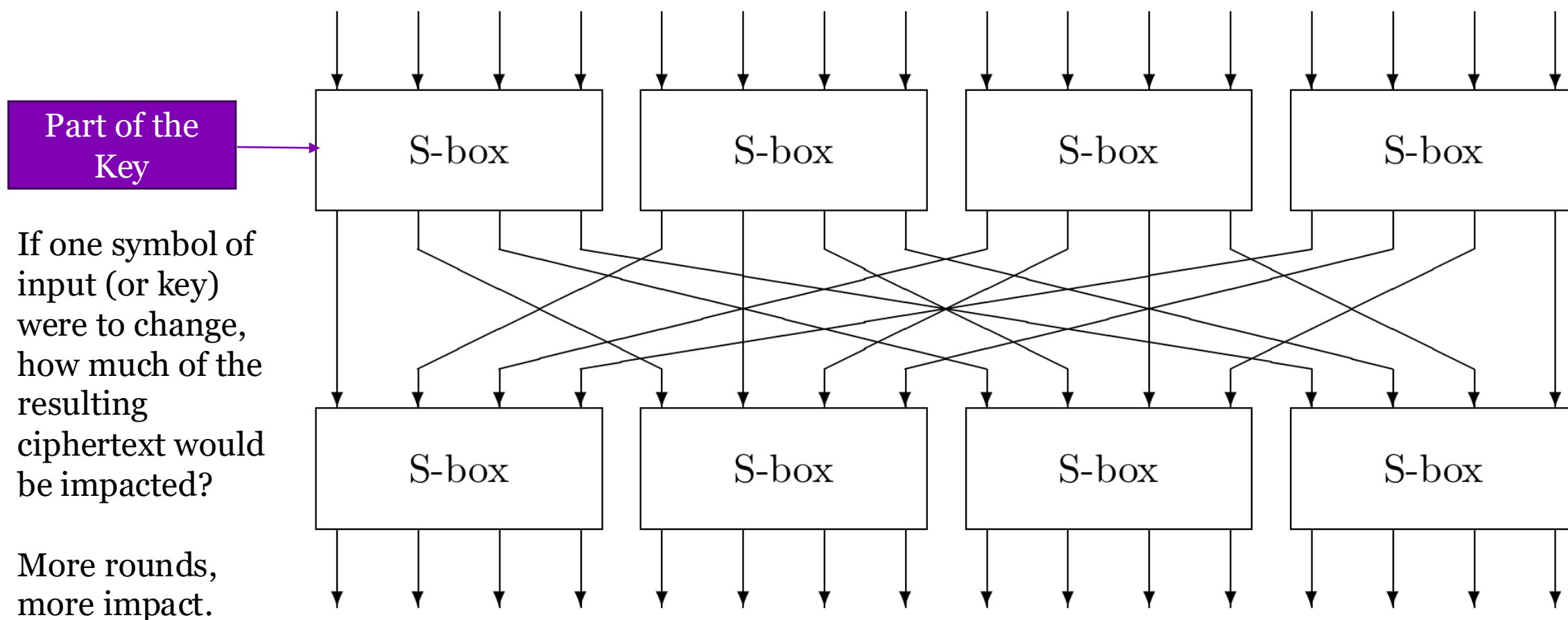
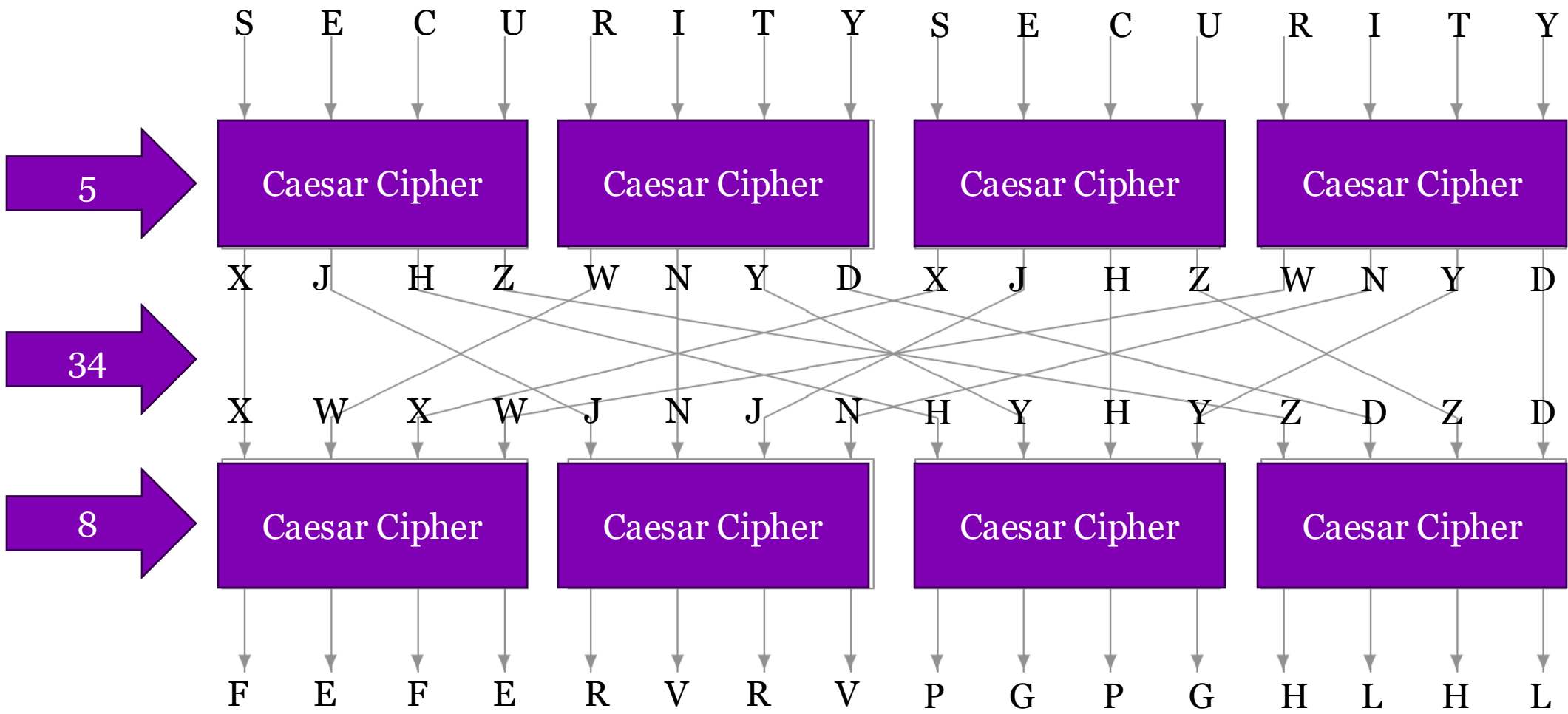


Figure 5.10: – a simple 16-bit SP-network block cipher

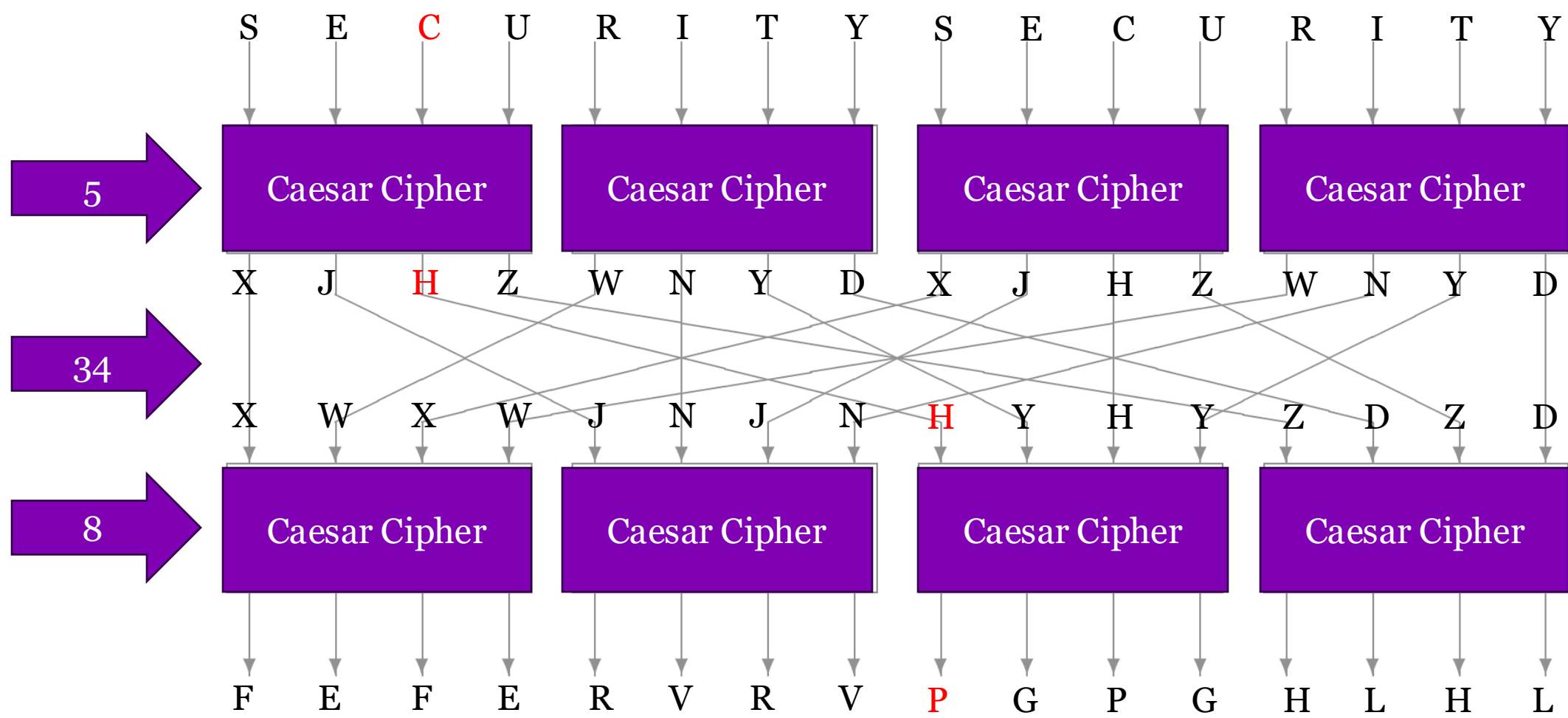
# SP-Networks: Simple Example

Key: 53489213



# SP-Networks: Simple Example

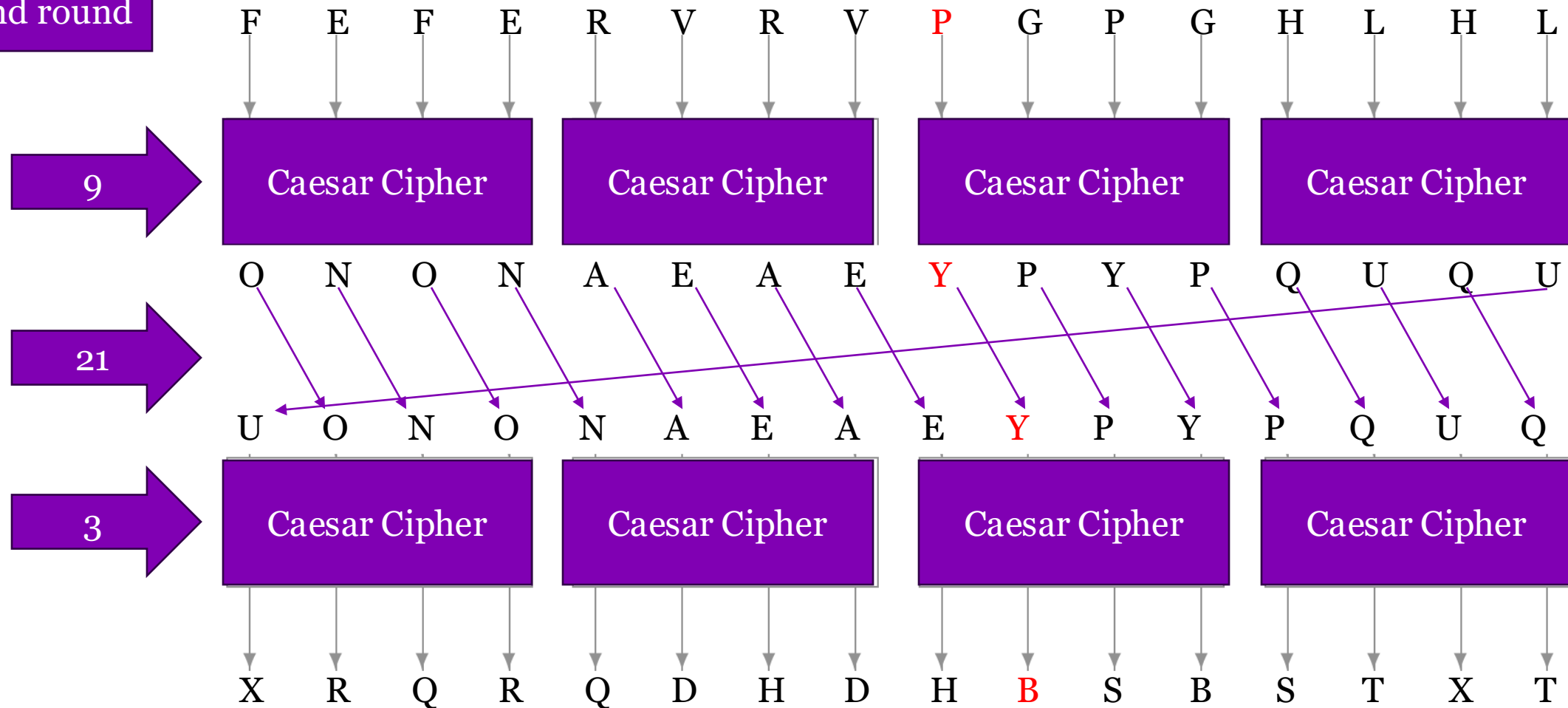
Key: 53489213



# SP-Networks: Simple Example

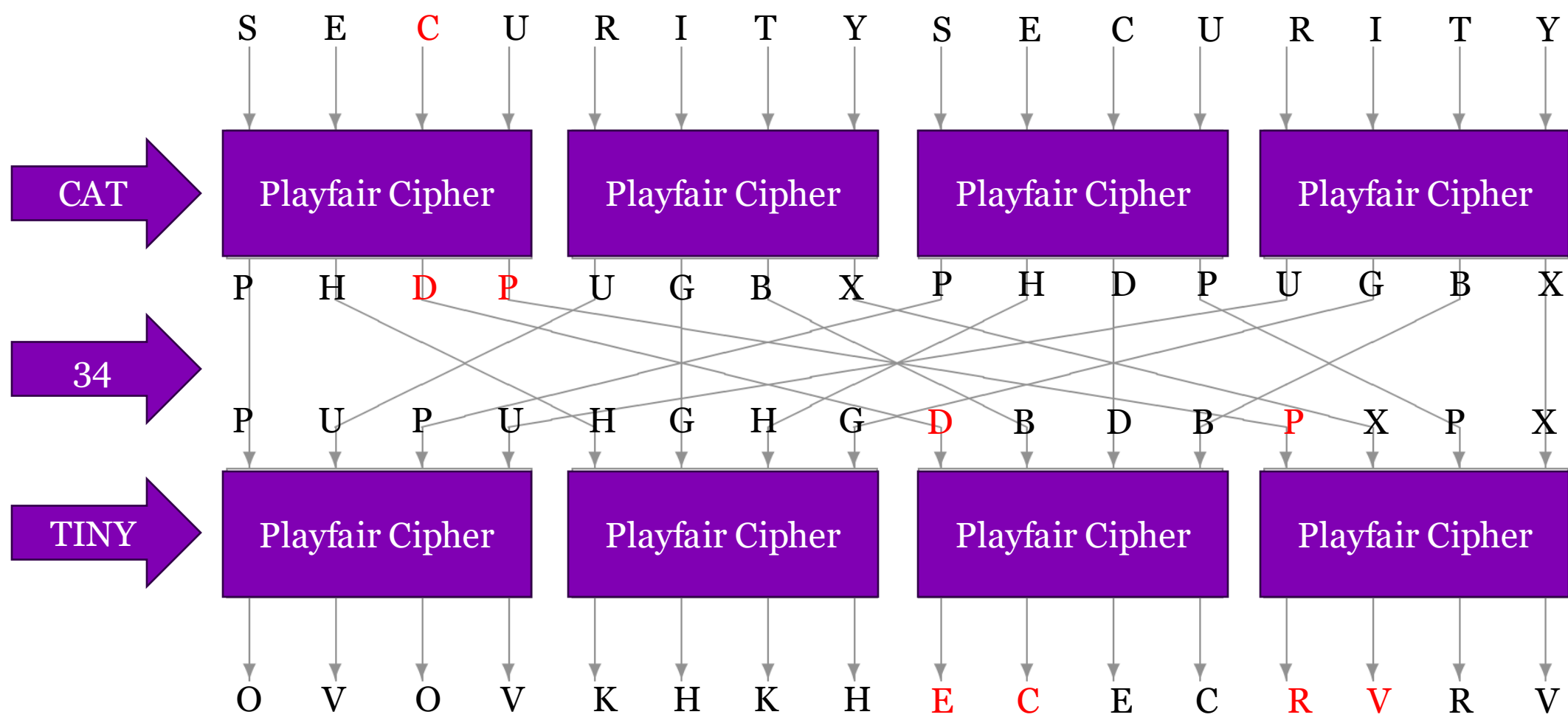
Key: 53489213

Second round



# SP-Networks: Simple Example

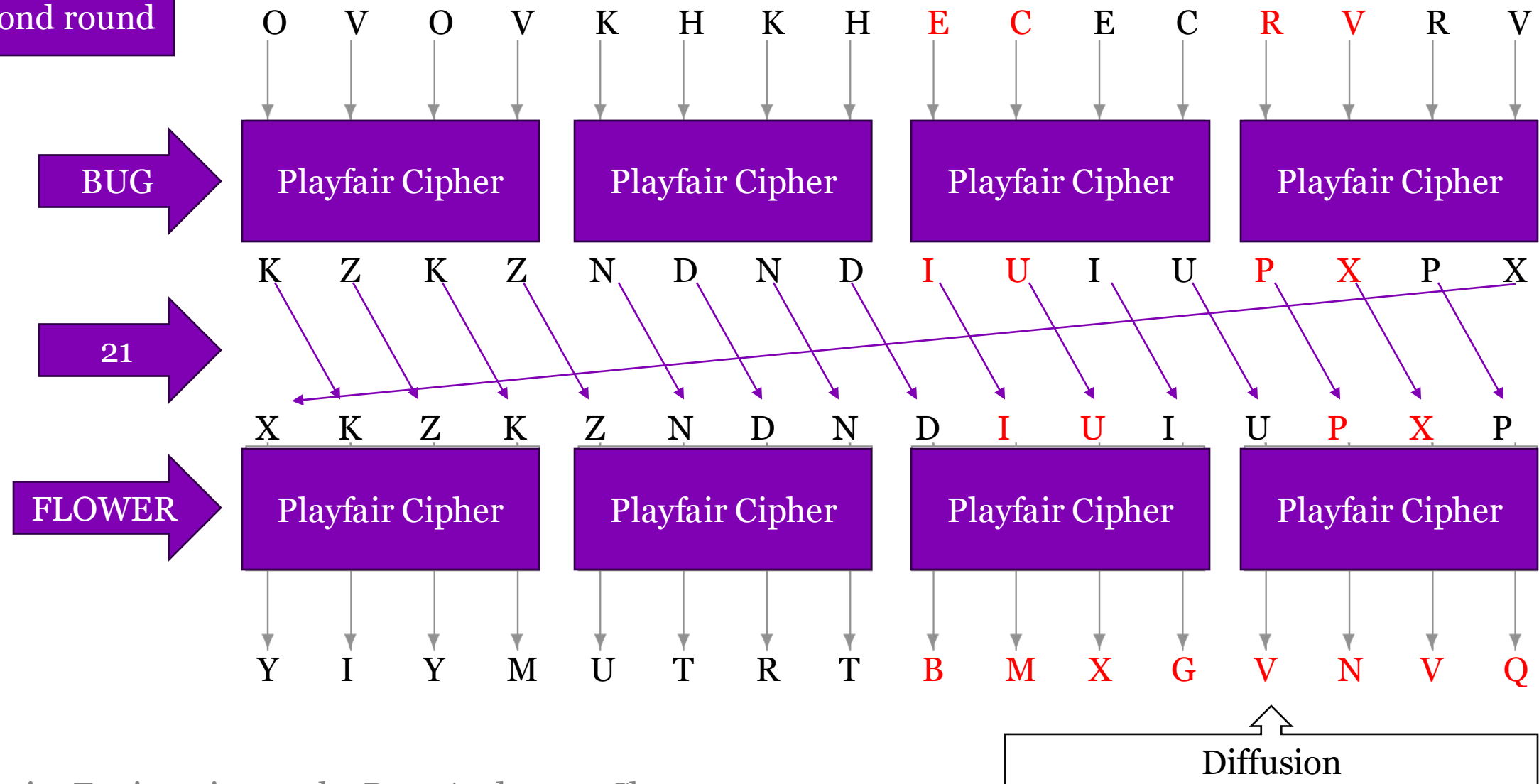
Key: CAT34TINYBUG21FLOWER



# SP-Networks: Simple Example

Key: CAT34TINYBUG21FLOWER

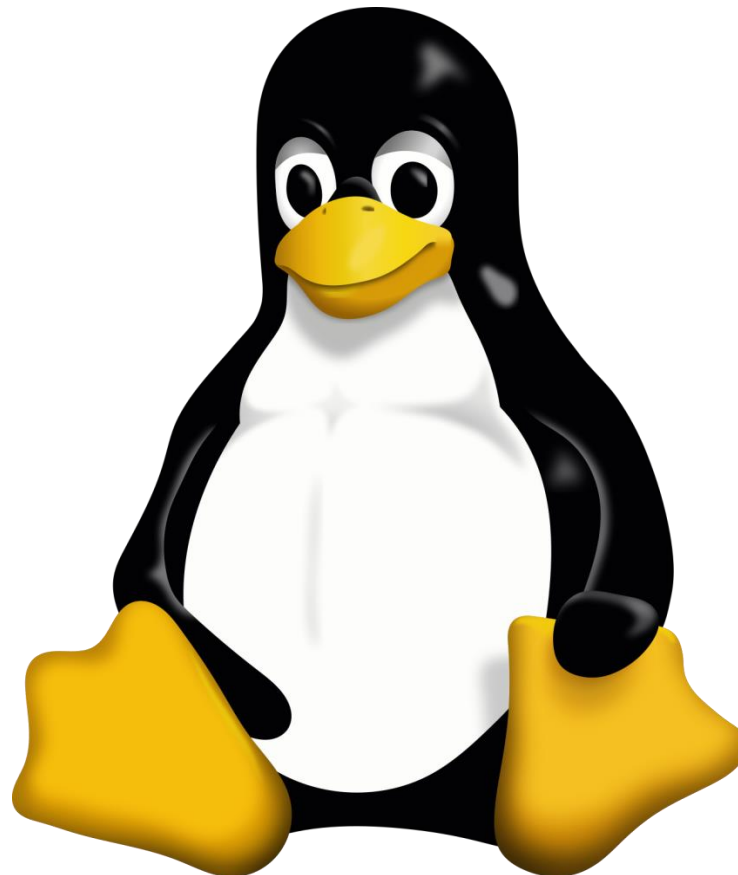
Second round



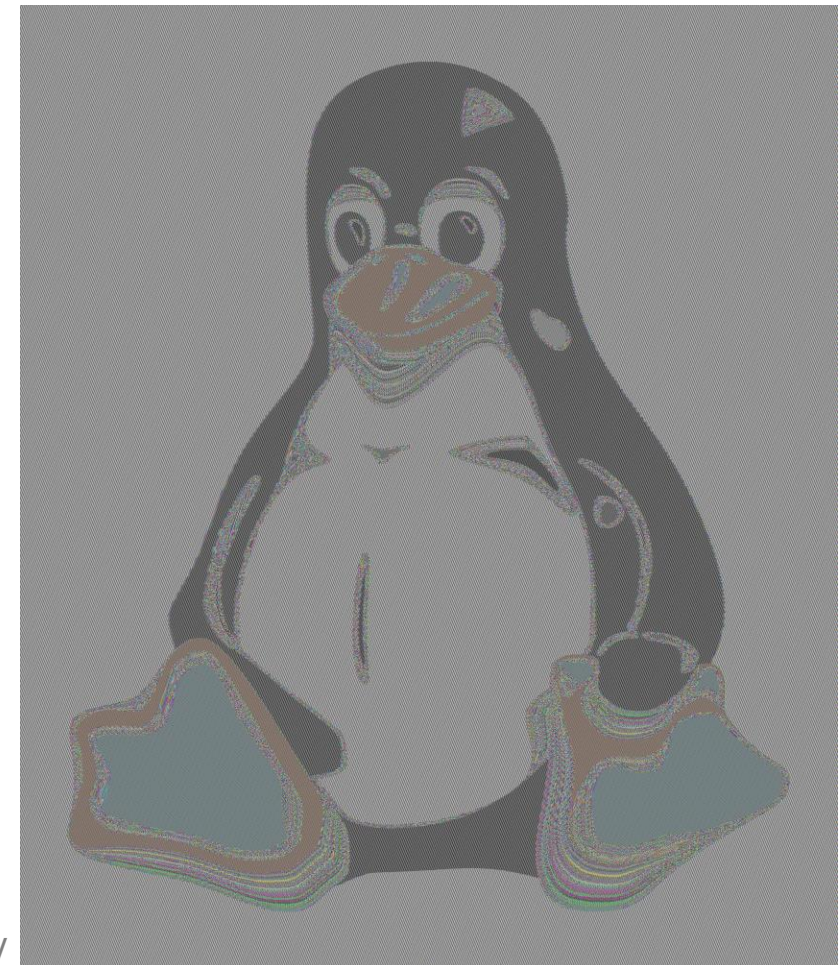
# ECB Penguin: what happens when block ciphers don't mix text between blocks

- Images are just binary text files so they can be encrypted
- Tux image has large blocks of solid color, scrambling the order of a block of nearly identical values does little
- Encrypted using AES-128 (Good crypto) using ECB (isolate blocks, bad idea)

Plaintext



Ciphertext



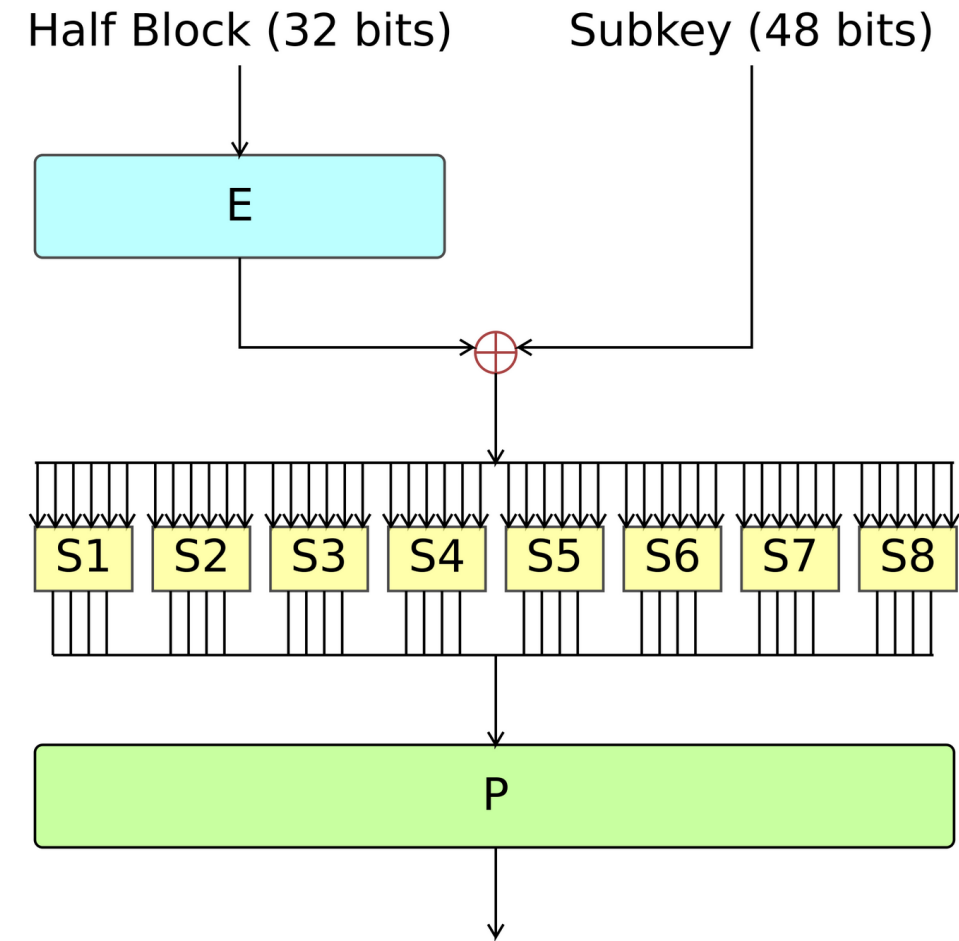
# Padding: Making a small thing bigger

- Playfair needs even number, so x might be added to end.
- Hash functions can be used to make a small string into a bigger one.

```
> sha256sum -t  
a  
  
87428fc522803d31065e7bce3  
cf03fe475096631e5e07bbd7a  
0fde60c4cf25c7
```

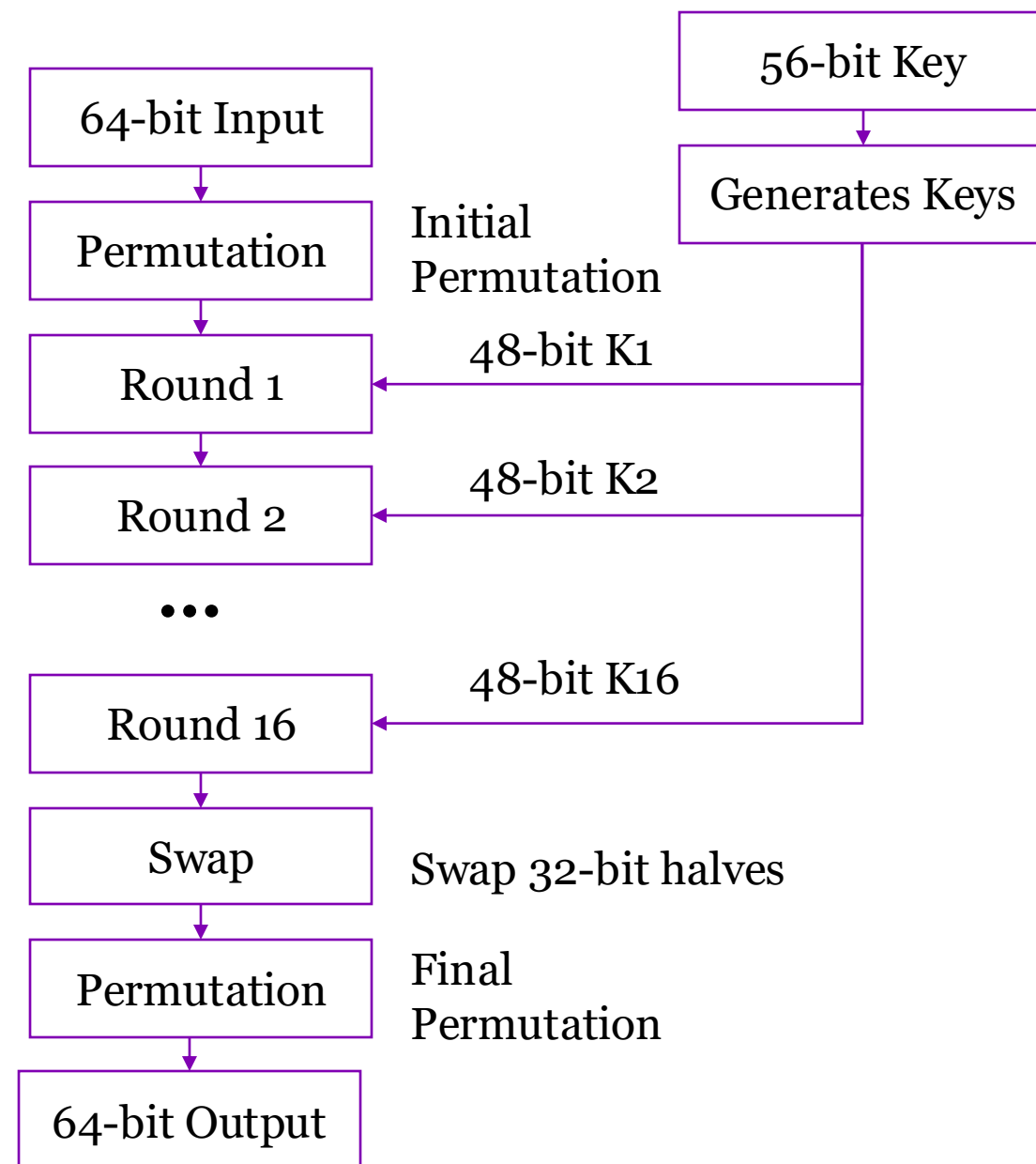
# Data Encryption Standard (DES)

- Symmetric-key algorithm using 56 bit keys (64 bit initial but 8 bits are parity)
- Blocks of 64 bits
- 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)



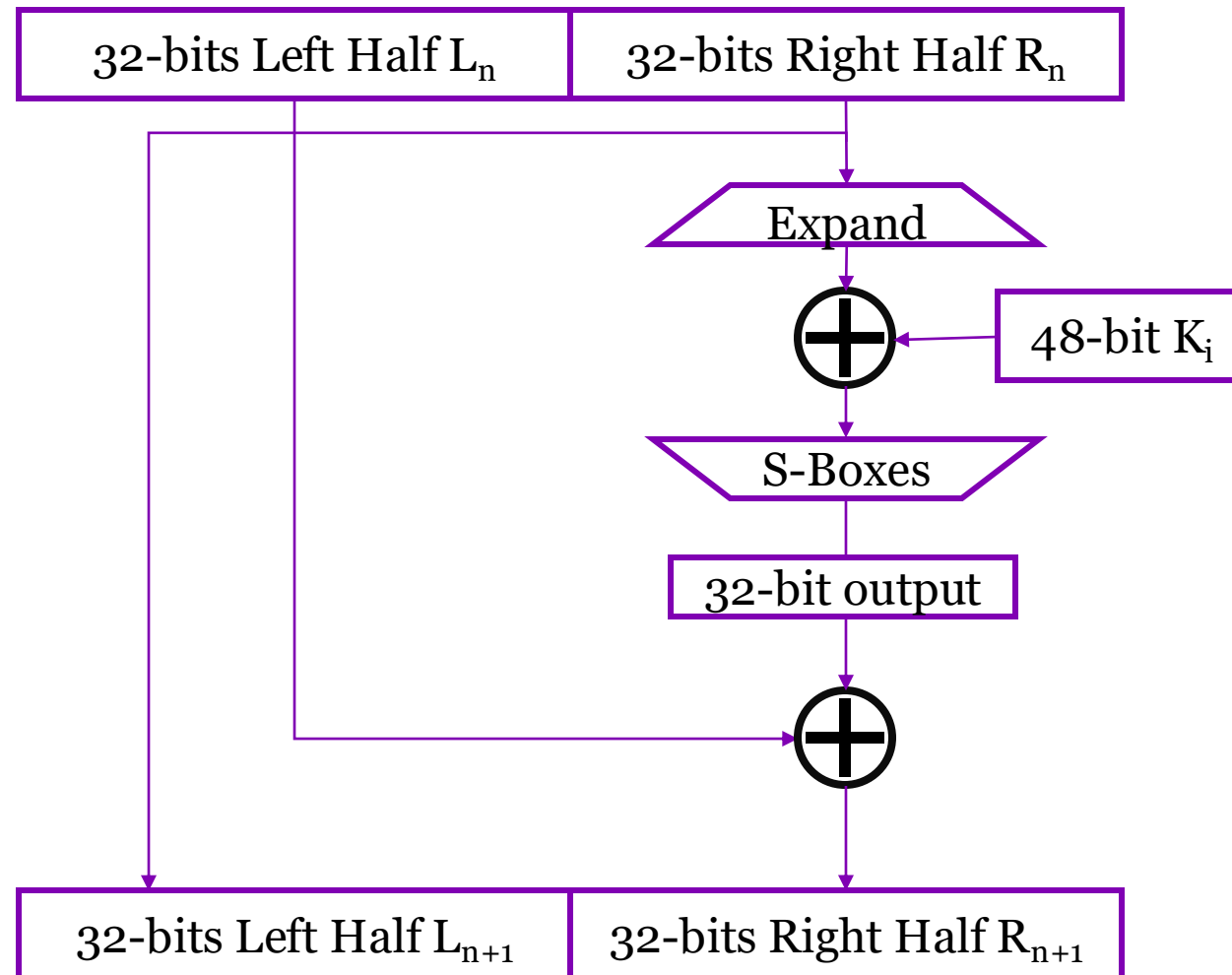
# Data Encryption Standard (DES)

- Symmetric-key algorithm using 56 bit keys (64 bit initial but 8 bits are parity)
- Blocks of 64 bits
- 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)



# Data Encryption Standard (DES)

- Each round
  - the ciphertext is divided in half.
  - Right half is expanded to 48 bits
  - XOR with the round key
  - S-boxes used to change back to 32-bit
  - XOR with the left half
  - Produces the new right half.

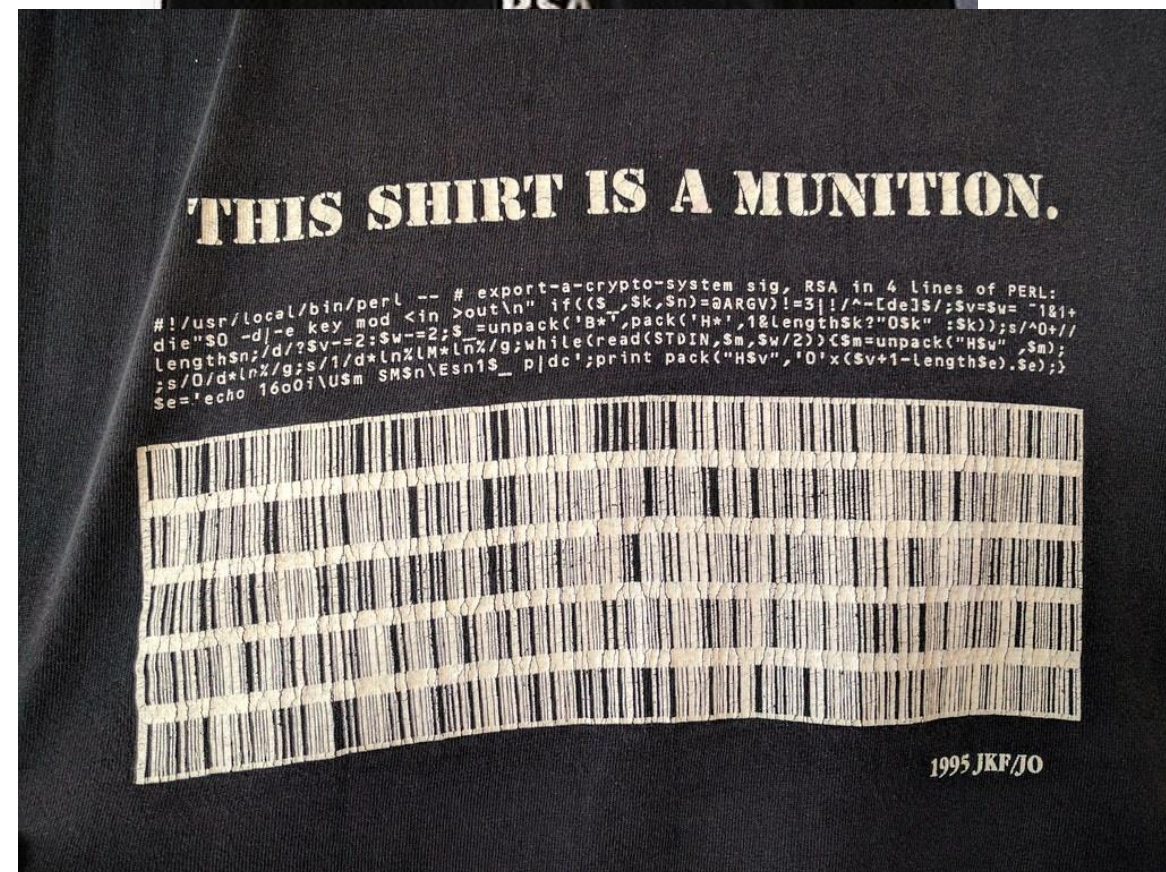
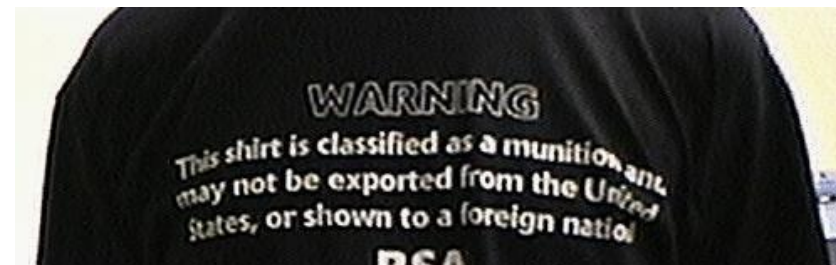


# Double and Tripple DES

- 56-bit (7-character) key is just too short
  - Idea: apply DES twice with two keys
  - $C = E(k_2, E(k_1, P))$
  - Unfortunately, this does little and creates roughly a 57-bit key strength
- Idea 2: apply DES three times
  - $C = E(k_3, E(k_2, E(k_1, P)))$
  - Gives roughly 112-bit key strength

# History: Crypto Wars

- Cold War era US export control restrictions on “munitions” including cryptography
- At end of WWII the military was the most common user of cryptography, so it was classified as a munition
- By the 1960’s though, finance started using crypto to protect wire transfers
- In 1975 DES released, but export outside US still limited



# History: Crypto Wars

- Early 90's PCs were now a thing and Netscape Navigator added SSL (https) encryption, but had to limit “international” edition to 40-bit keys instead of 128-bit
- By late 90's there were various lawsuits and complaints about how weak encryption was limiting sales and growth of e-commerce
- Bill Clinton signed order in 1996 removing encryption from munitions list and declaring software to not be a “technology”



# Crypto Wars 2.0: Going Dark

- Ongoing balance debate on how to best “protect” citizens
- Protect: Allow police to look at everyone’s stuff (hopefully with warrant) to look for bad things
- Protect: Defend against anyone seeing information without authorization



## Crypto Wars 2.0: How Should The U.S. Balance Privacy and National Security?

March 12, 2015

Event

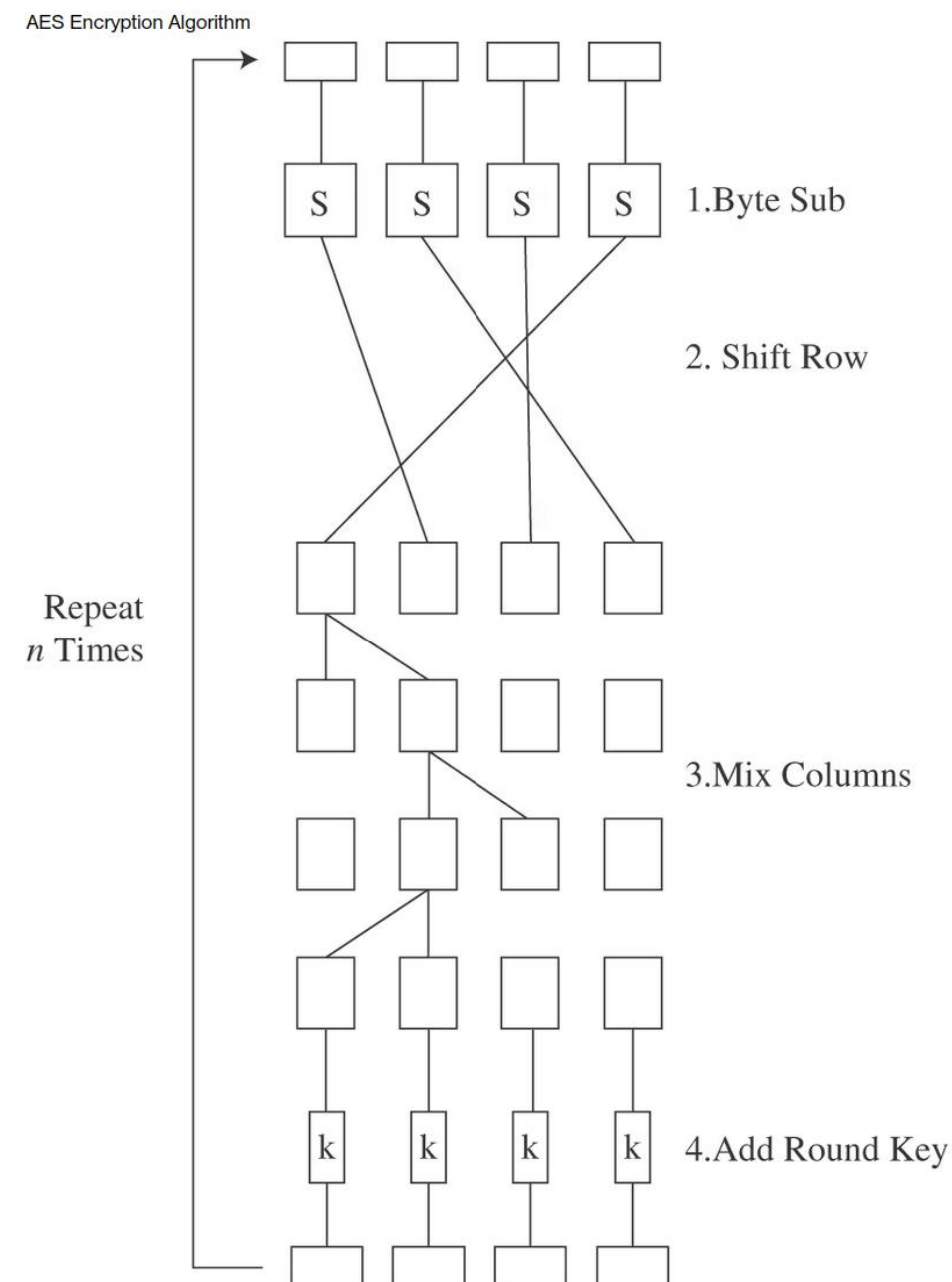
President Barack Obama, British Prime Minister David Cameron, and Chinese President Xi Jinping, among other world leaders, have suggested that companies should not create IT products and services so secure that governments cannot gain access. FBI Director James Comey has gone so far as to criticize companies that build consumer devices designed without back doors for law enforcement, and one Justice Department official has labeled devices with strong encryption a “zone of lawlessness.” These statements reflect a deep disconnect between ongoing efforts, including within the federal government, to build ever more secure systems for data and attempts by the intelligence community and law enforcement to circumvent them. The tension also reflects a significant threat to the future economic success of the U.S. tech industry, since foreign competitors are likely to offer more secure alternatives in the global market.

While the Crypto Wars of the 1990’s may be over, there are clearly more battles ahead. Join ITIF for a panel to discuss how these proposed policies will affect consumers’ privacy and security, the implications for the U.S. tech sector, and alternative policy options that might strike a better balance the needs of law enforcement and robust security practices.

**Friday Lecture stopped here**

# Advanced Encryption System (AES)

- Became a standard in the US in 2001
- Primarily uses substitution, transposition, the shift, exclusive OR, and addition
- Can use 128, 192, 256 bit keys, and larger keys are possible



# QUESTIONS