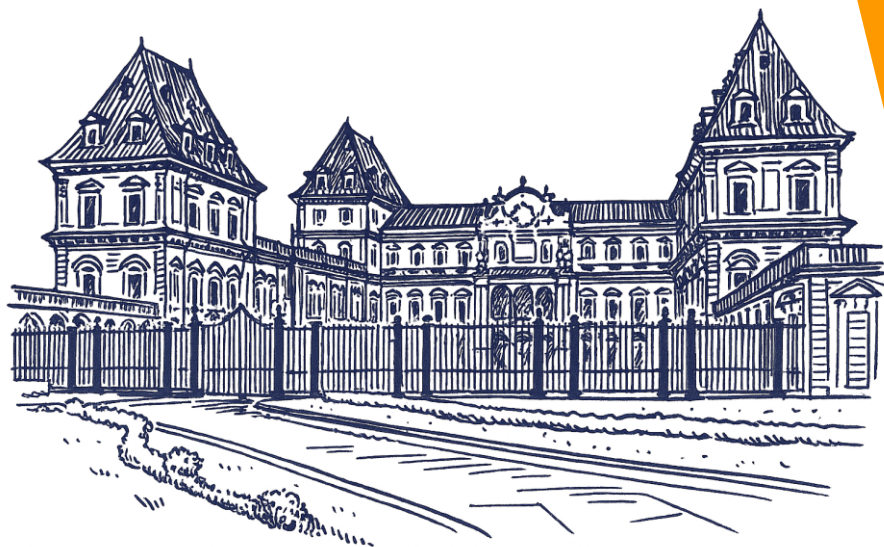




A Tale of Errors and Secrets

Leonardo Errati



Politecnico
di Torino

CrypTO



FANNY



ARTHUR



CORALINE



HIPPOLYTE



GWEN



AUGUSTIN



MAGGIE



ROGER



MARTIN



THEOPHILE



CAPUCINE



MAXIME



MELINA



ROBIN



SANDRA

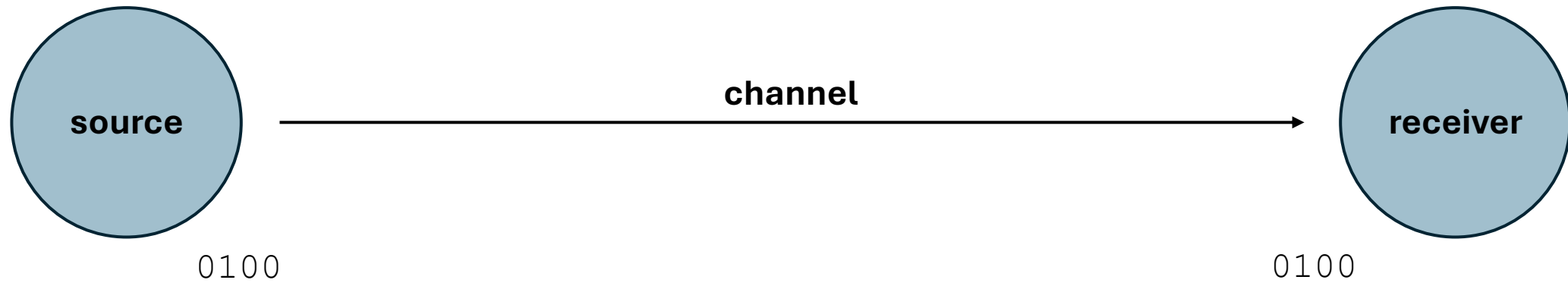


JUSTINE

The background is a solid dark blue. In the upper left, there is a stylized illustration of a classical building with multiple stories, arched windows, and a central entrance. Above the building, on the left, is a profile of a person wearing a classical helmet with a plume, holding a spear. On the right side, there are stylized leafy branches. At the bottom center, the year '1850' is partially visible.

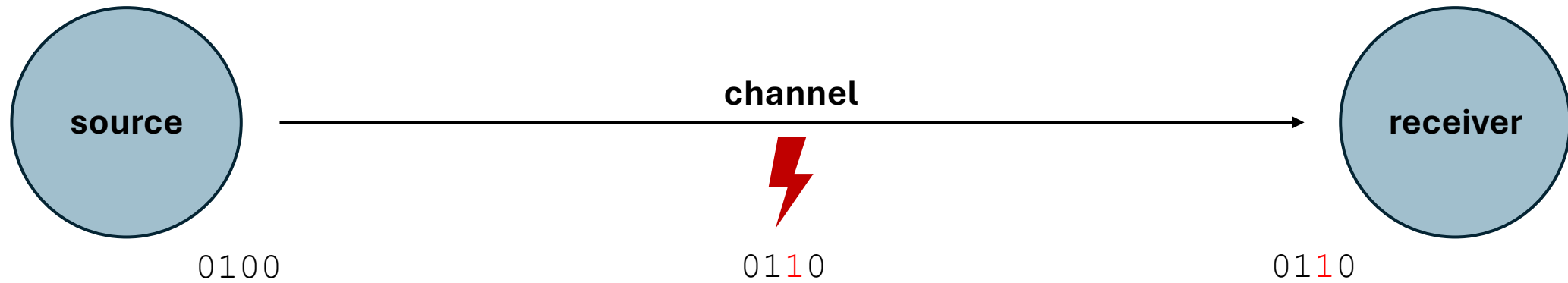
1: CODING THEORY

Coding theory



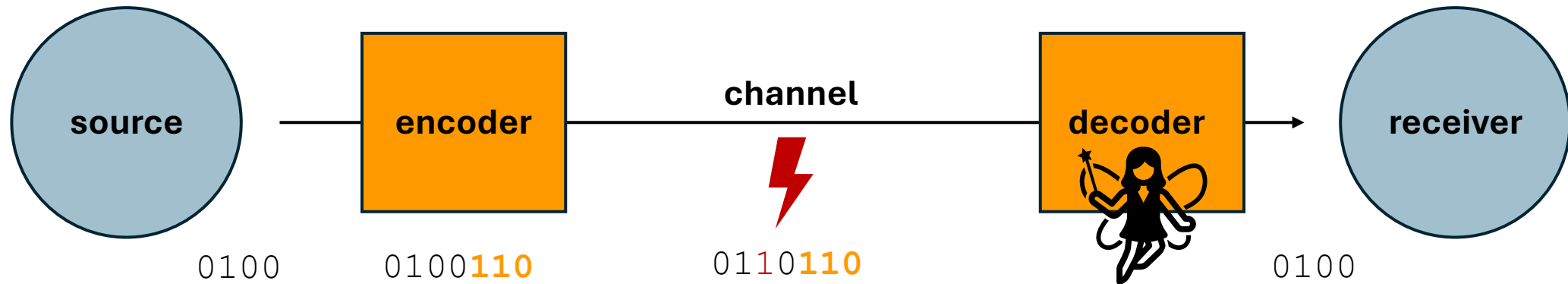
A alphabet
 k input length

Coding theory



A alphabet
 k input length

Coding theory



A alphabet
 k input length
 n code length

Coding theory



Hackaday

Cosmic Ray Flips Bit, Assists Mario 64 Speedrunner

The leading theory is that this bit flip was caused by a cosmic ray event, though the likelihood of such an event is exceedingly rare. It's...

17 feb 2021



BBC

Bit flips: How cosmic rays grounded a fleet of aircraft

Radiation from space that led to more than 6000 Airbus aircraft needing emergency computer updates could become a growing problem.

1 dic 2025



*“around one error per month per 256 MiB of RAM on a desktop computer”
(IBM, 1996)*

Codes

A **code** is a map $\varphi: S^k \rightarrow S^n$.

We want it to

- be easy to invert
- be easy to memorise
- be efficient

$$\varphi: (x_1, x_2, x_3, x_4) \rightarrow ?$$

Codes

A **code** is a map $\varphi: S^k \rightarrow S^n$.

We want it to

- be easy to invert
- be easy to memorise
- be efficient

$$\varphi: (x_1, x_2, x_3, x_4) \rightarrow (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$$

$$x_5 = f(x_1, x_2, x_3, x_4)$$

$$x_6 = f(x_1, x_2, x_3, x_4)$$

$$x_7 = f(x_1, x_2, x_3, x_4)$$

Linear codes

$$\varphi: (x_1, x_2, x_3, x_4) \rightarrow (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$$

$$x_5 = x_1 + x_2 + x_4$$

$$x_6 = x_1 + x_3 + x_4$$

$$x_7 = x_2 + x_3 + x_4$$

Linear codes

A **linear code** is $C = \{xG : x \in S^k\}$.

The matrix is called **generator matrix**.

Usually $S = F_q$, so C is a linear subspace of F_q^n .

$$\varphi: (x_1, x_2, x_3, x_4) \rightarrow (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$$

$$x_5 = x_1 + x_2 + x_4$$

$$x_6 = x_1 + x_3 + x_4$$

$$x_7 = x_2 + x_3 + x_4$$

$$(x_1, x_2, x_3, x_4) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$$

Linear codes

Our constraints form a system of equations.

$$\begin{cases} x_1 + x_2 + x_4 + x_5 = 0 \\ x_1 + x_3 + x_4 + x_6 = 0 \\ x_2 + x_3 + x_4 + x_7 = 0 \end{cases}$$

$$x_5 = x_1 + x_2 + x_4$$

$$x_6 = x_1 + x_3 + x_4$$

$$x_7 = x_2 + x_3 + x_4$$

All elements of C satisfy it. This defines the **parity check matrix**, H .

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Linear codes

From generator G :

- The code is $C = \langle G \rangle$
- k linearly independent rows
- n columns

$$m \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = c$$

From parity check H :

- The code is $C = \ker(H)$
- $n - k$ linearly independent rows
- n columns

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} c^T = 0$$

Linear codes

From generator G :

- The code is $C = \langle G \rangle$
- k linearly independent rows
- n columns

From parity check H :

- The code is $C = \ker(H)$
- $n - k$ linearly independent rows
- n columns


$$m \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = c$$
$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} c^T = 0$$

Linear codes

From generator G :

- The code is $C = \langle G \rangle$
- k linearly independent rows
- n columns

From parity check H :

- The code is $C = \ker(H)$
- $n - k$ linearly independent rows
- n columns

$$m \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = c \quad \longleftrightarrow \quad \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} c^T = 0$$

Theorem.

If $G = (I_k \mid A)$, then $H = (-A^T \mid I_{n-k})$.

Linear codes

Some codes are more equal than others.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Theorem.

If $G = (I_k \mid A)$, then $H = (-A^T \mid I_k)$.

Linear codes

Some codes are more equal than others.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

systematic form



$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

permuted systematic

Theorem.

If $G = (I_k \mid A)$, then $H = (-A^T \mid I_k)$.

Linear codes

Some codes are more equal than others.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

systematic form



$$G' = GP$$

permuted systematic

Theorem.

If $G = (I_k \mid A)$, then $H = (-A^T \mid I_k)$.

Linear codes

Some codes are more equal than others.

permutation equivalent
permutation equivalent (2)

$$G' = GP$$
$$G' = SGP$$

Linear codes

Some codes are more equal than others.

permutation equivalent

permutation equivalent (2)

linearly equivalent

$$G' = GP$$

$$G' = SGP$$

$$G' = SGPD$$

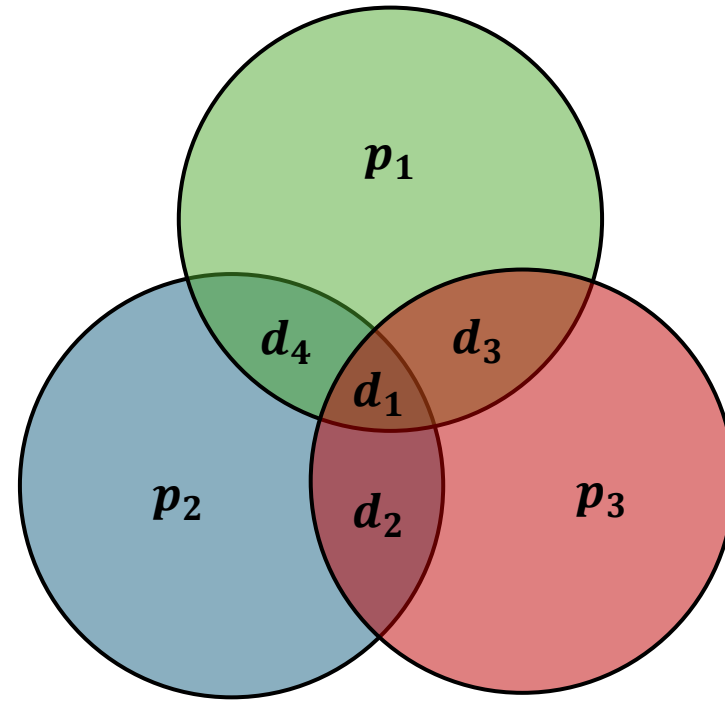
Linear codes

0	0000 000
1	0001 011
2	0010 101
3	0011 110
4	0100 110
5	0101 101
6	0110 011
7	0111 000
8	1000 111
9	1001 100
10	1010 010
11	1011 001
12	1100 001
13	1101 010
14	1110 100
15	1111 111

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Linear codes

0	0000 000
1	0001 011
2	0010 101
3	0011 110
4	0100 110
5	0101 101
6	0110 011
7	0111 000
8	1000 111
9	1001 100
10	1010 010
11	1011 001
12	1100 001
13	1101 010
14	1110 100
15	1111 111



$$p_1 = d_1 + d_2 + d_4$$

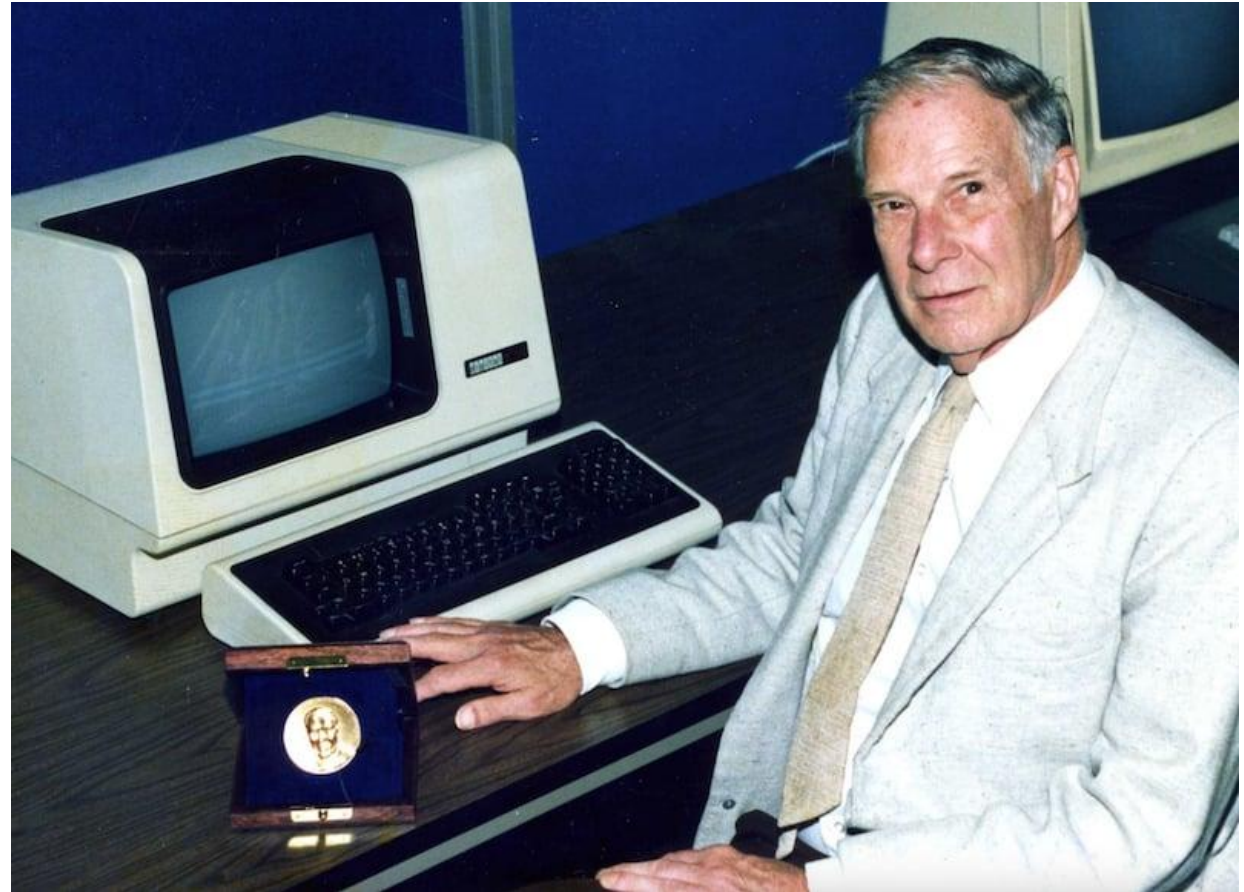
$$p_2 = d_1 + d_3 + d_4$$

$$p_3 = d_2 + d_3 + d_4$$

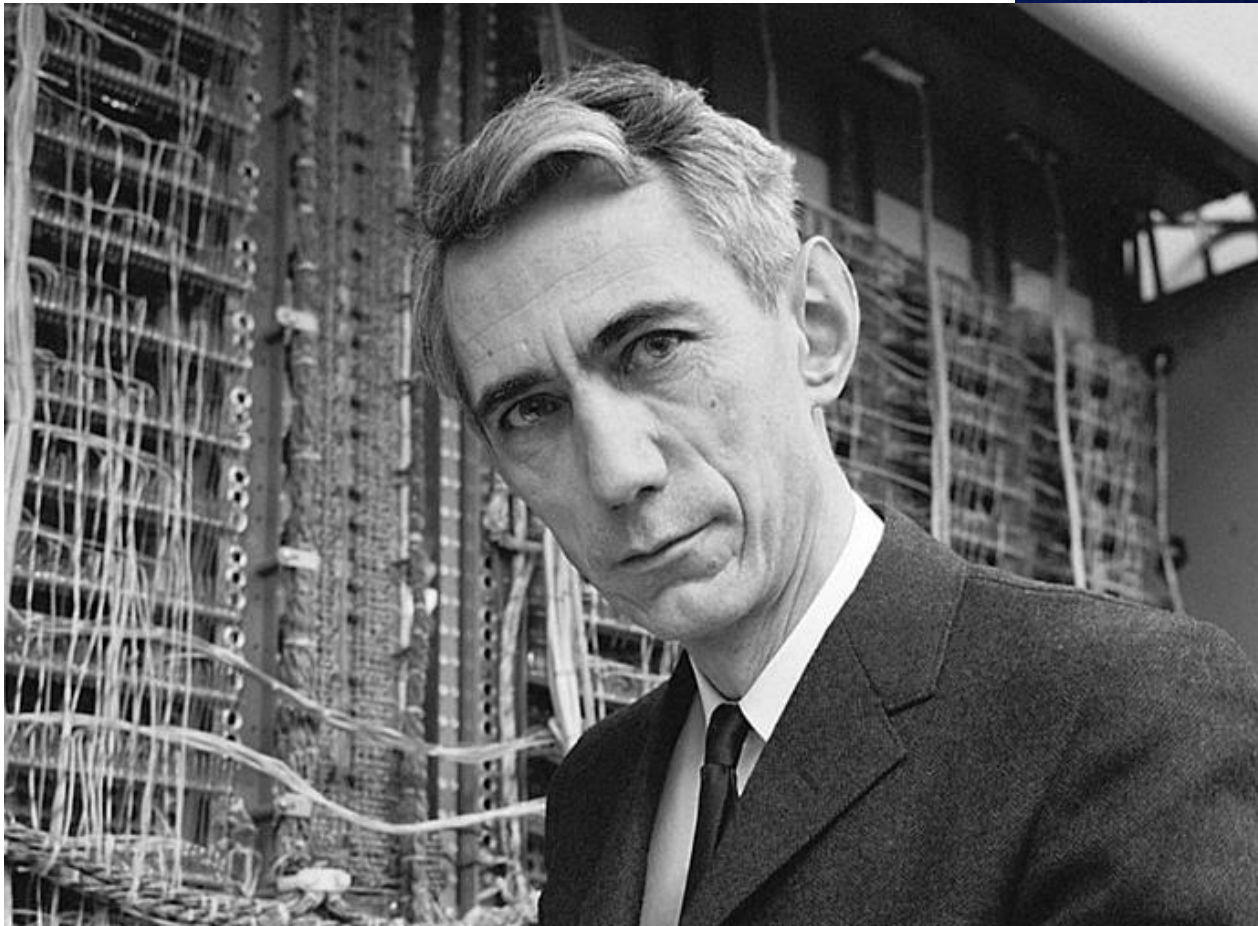
Linear codes

0	0000	000
1	0001	011
2	0010	101
3	0011	110
4	0100	110
5	0101	101
6	0110	011
7	0111	000
8	1000	111
9	1001	100
10	1010	010
11	1011	001
12	1100	001
13	1101	010
14	1110	100
15	1111	111

[7,4] Hamming code



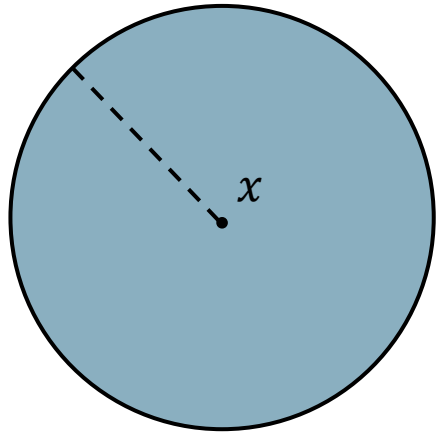
Linear codes



How to decode?

The **Hamming weight** of a codeword is $w_H(x) = \#\{i : x_i \neq 0\}$.

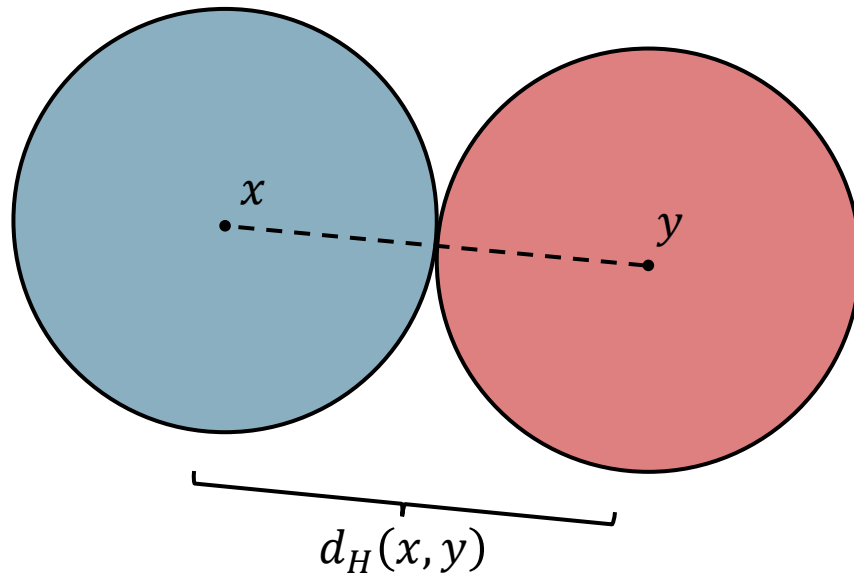
The **Hamming distance** of x, y is $d_H(x, y) = w_H(x - y)$.



How to decode?

The **Hamming weight** of a codeword is $w_H(x) = \#\{i : x_i \neq 0\}$.

The **Hamming distance** of x, y is $d_H(x, y) = w_H(x - y)$.

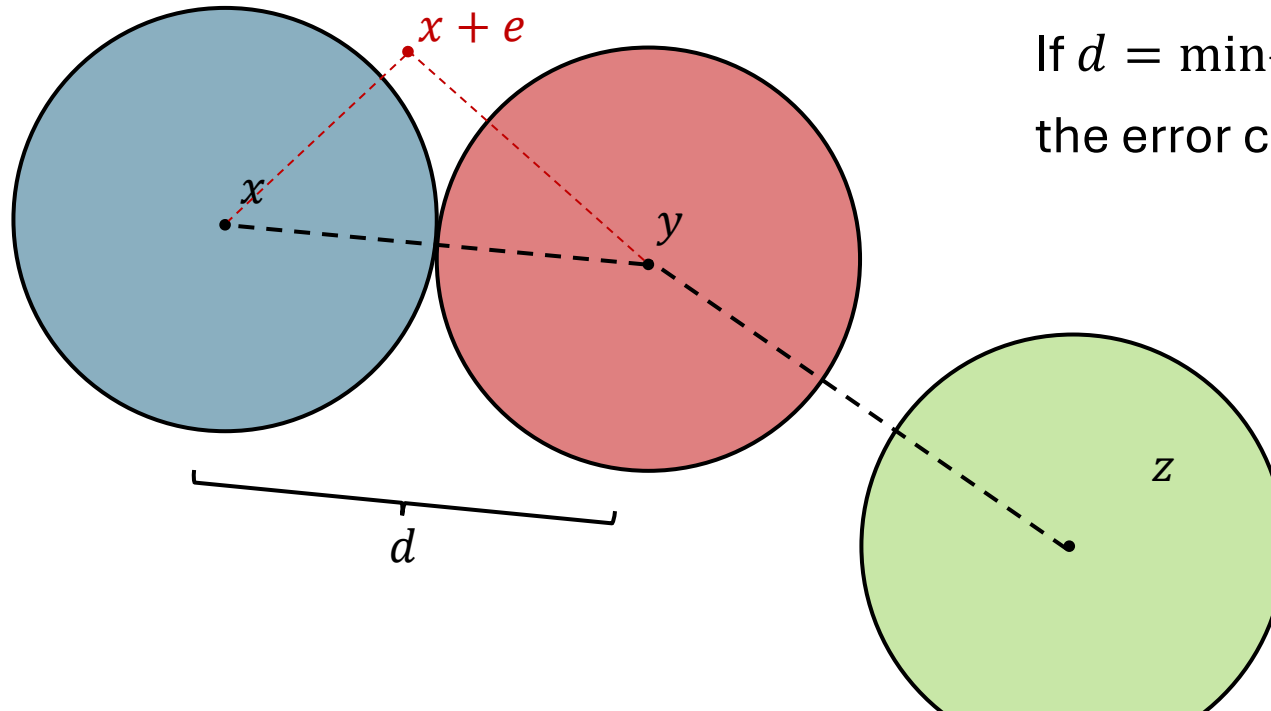


How to decode?

Nearest neighbour decoding.

Receive $x + e$, for $x \in C$ and e error.

Return the $c \in C$ closest to $x + e$.



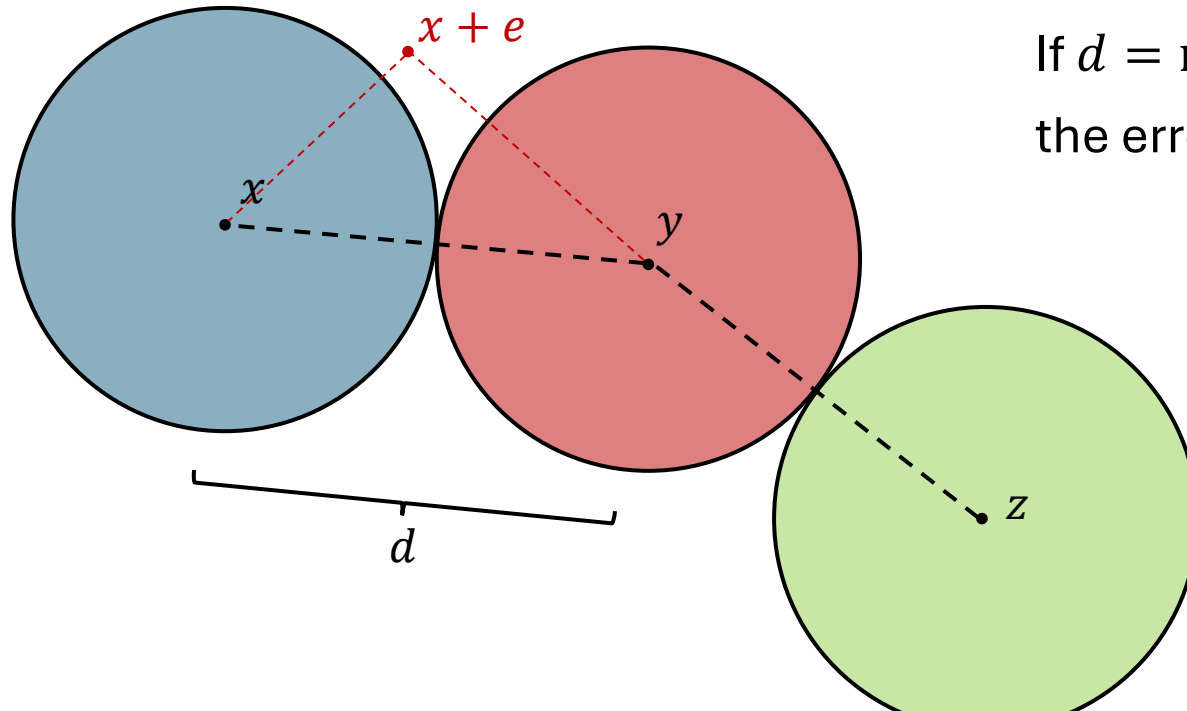
If $d = \min\{d_H(x, y) : x, y \in C\}$,
the error correction capacity is $\left\lfloor \frac{d-1}{2} \right\rfloor$.

How to decode?

Nearest neighbour decoding.

Receive $x + e$, for $x \in C$ and e error.

Return the $c \in C$ closest to $x + e$.



If $d = \min\{d_H(x, y) : x, y \in C\}$,
the error correction capacity is $\left\lfloor \frac{d-1}{2} \right\rfloor$.

How to decode?

Nearest neighbour decoding.

Receive $x + e$, for $x \in \mathcal{C}$ and e error.

Return the $c \in \mathcal{C}$ closest to $x + e$.

Theorem (Singleton Bound).

If d is the minimum distance of an $[n, k]$ -code, $d \leq n - k + 1$.

How to decode?

Syndrome decoding.

Receive $x + e$, for $x \in C$ and e error. Then

$$H(x + e)^T = Hx^T + He^T = He^T$$

How to decode?

Build a table of all $n - k$ cosets of form $e + C$.

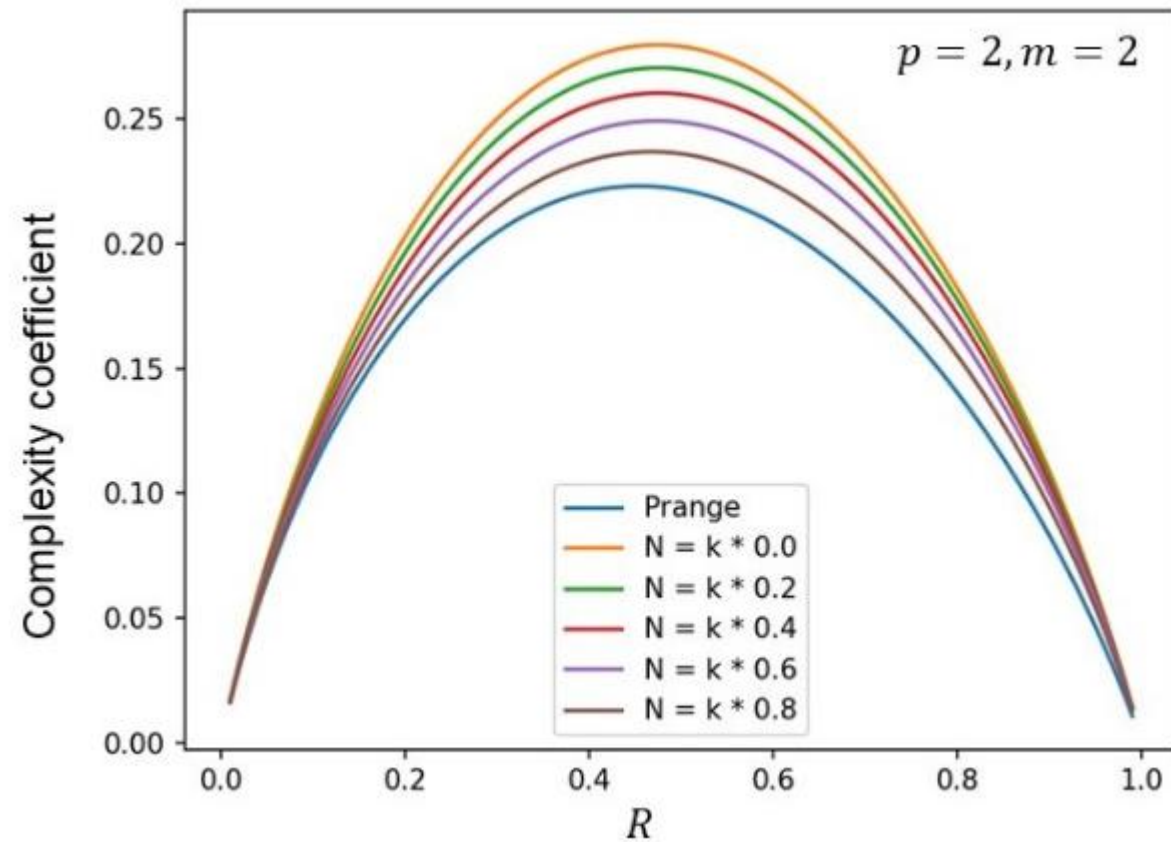
0000000		0000000	0001111	0010011	0011100	0100101	0101010	0110110	0111001	1000110	1001001	1010101	1011010	1100011	1101100	1110000	1111111
0000001		0000001	0001110	0010010	0011101	0100100	0101011	0110111	0111000	1000111	1001000	1010100	1011011	1100010	1101101	1110001	1111110
0000010		0000010	0001101	0010001	0011110	0100111	0101000	0110100	0111011	1000100	1001011	1010111	1011000	1100001	1101110	1110010	1111101
0000100		0000100	0001011	0010111	0011000	0100001	0101110	0110010	0111101	1000010	1001101	1010001	1011110	1100111	1101000	1110100	1111011
0001000		0001000	0000111	0011011	0010100	0101101	0100010	0111110	0110001	1001110	1000001	1011101	1010010	1101011	1100100	1111000	1110111
0010000		0010000	0011111	0000011	0001100	0110101	0111010	0100110	0101001	1010110	1011001	1000101	1001010	1110011	1111100	1100000	1101111
0100000		0100000	0101111	0110011	0111100	0000101	0001010	0010110	0011001	1100110	1101001	1110101	1111010	1000011	1001100	1010000	1011111
1000000		1000000	1001111	1010011	1011100	1100101	1101010	1110110	1111001	0000110	0001001	0010101	0011010	0100011	0101100	0110000	0111111

Find the coset of e via the syndrome.

Pick as candidate for e the element of lowest weight.

How to decode?

For a random code...



Behind the trick

Goal. Build codewords c such that

$$Hc^T = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} c^T = 0$$

Behind the trick

Goal. Build codewords c such that

$$Hc^T = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} c^T = 0$$

1. Identify 7 *independent* characteristics.
2. Use the generator matrix, it's easier.
3. For every codeword c , generate the individual using them.



CAPUCINE

1010

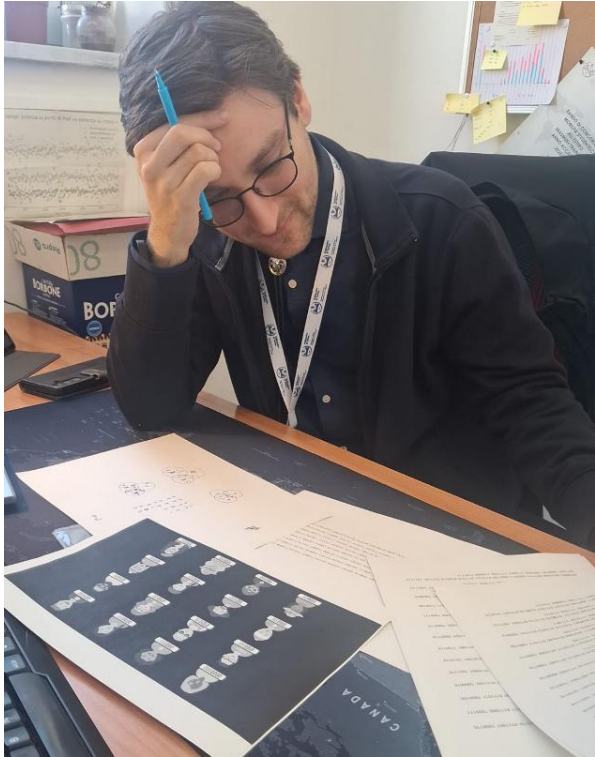


CAPUCINE

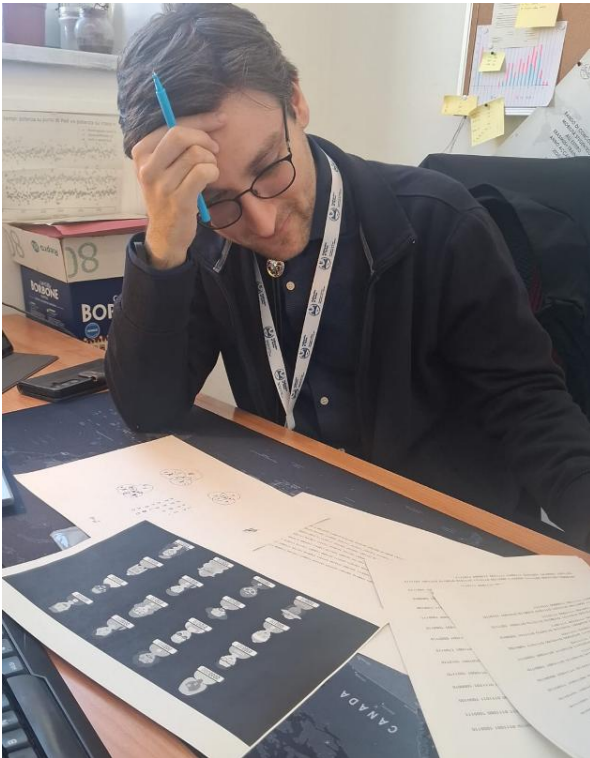
1010101



Behind the trick

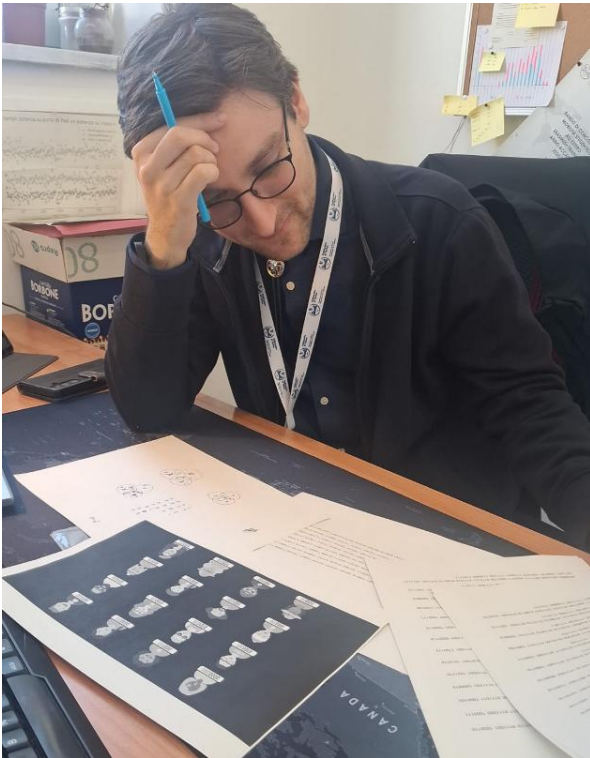


Behind the trick



```
answer with 'y' for Yes or 'n' for No:  
1. Hat? 1  
2. Glasses? 0  
3. Is sad? 1  
4. Moustache? 0  
5. Drawing on shirt? 1  
6. Blue shirt/garment? 1  
7. Dark hair? 1  
Lie detected at question 6!  
Identified Person: CAPUCINE  
  
Do you want to play again? (y/n):
```

Behind the trick



answer with 'y' for Yes or 'n' for No:

1. Hat? 1
2. Glasses? 0
3. Is sad? 1
4. Moustache? 0
5. Drawing on shirt? 1
6. Blue shirt/garment? 1
7. Dark hair? 1

Lie detected at question 6!
Identified Person: CAPUCINE

Do you want to play again? (y/n):

The background is a solid dark blue. In the upper left, there is a stylized illustration of a classical building with multiple stories, arched windows, and a central entrance. Above the building, on the left, is a profile of a person wearing a classical helmet with a plume, holding a spear. On the right side, there are stylized leafy branches. At the bottom center, the year '1850' is partially visible.

2: CRYPTOGRAPHY

Atbash cipher

*“And after all of them, the king of
Sheshak will drink it too.”*

(Book of Jeremiah, 25:26)

Sheshak
shin-shin-kaf

22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
Tav	Shin	Reish	Qof	Tsadé	Pé	Ayin	Samekh	Noun	Meme	Lamed	Kaf	Yod	Teith	Heith	Zayin	Vav	Hé	Dalet	Guimel	Beith	Alpeh

Atbash cipher

“And after all of them, the king of **Sheshak** will drink it too.”

(Book of Jeremiah, 25:26)

Sheshak
shin-shin-kaf $\xrightarrow{\varphi_{\text{atbash}}}$ bet-bet-lamed

22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
Tav	Shin	Reish	Qof	Tsadé	Pé	Ayin	Samekh	Noun	Meme	Lamed	Kaf	Yod	Teith	Heith	Zayin	Vav	Hé	Dalet	Guimel	Beith	Alpeh

$$\begin{aligned}\varphi_{\text{atbash}}: \mathbb{Z}_{22} &\rightarrow \mathbb{Z}_{22} \\ x &\mapsto (23 - x) \bmod 22\end{aligned}$$

Atbash cipher

“And after all of them, the king of **Sheshak** will drink it too.”

(Book of Jeremiah, 25:26)

Sheshak
shin-shin-kaf

φ_{atbash}

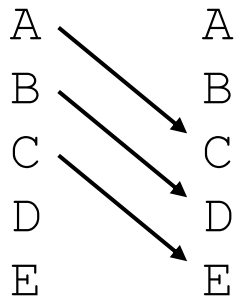
Babylon
bet-bet-lamed

22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
Tav	Shin	Reish	Qof	Tsadé	Pé	Ayin	Samekh	Noun	Meme	Lamed	Kaf	Yod	Teith	Heith	Zayin	Vav	Hé	Dalet	Guimel	Beith	Alpeh

$$\begin{aligned}\varphi_{\text{atbash}}: \mathbb{Z}_{22} &\rightarrow \mathbb{Z}_{22} \\ x &\mapsto (23 - x) \bmod 22\end{aligned}$$

Caesar cipher

$$\begin{aligned}\varphi_{caesar}: \mathbb{Z}_{26} &\rightarrow \mathbb{Z}_{26} \\ x &\mapsto (x + k) \bmod 26\end{aligned}$$



message: ATTACKATDAWN
key: C
ciphertext: DWWDFNDWGDZQ

$$H(K) = - \sum_{k \in K} P[k] \cdot \log_2 P[k]$$

$$H_{caesar} \simeq 4.7$$

Vigenere cipher

$$k = (k_0, \dots, k_{t-1})$$

$$\begin{aligned} \varphi_{\text{vigenere}}: \mathbb{Z}_{26} &\rightarrow \mathbb{Z}_{26} \\ x &\mapsto (x_i + k_{i \bmod t}) \bmod 26 \end{aligned}$$

message:	ATTACKATDAWN
key:	keykeykeykey
ciphertext:	KXRKGIKXBYAL

$$H_{\text{vigenere}} \simeq 4.7 \cdot t$$

Vigenere cipher

$$k = (k_0, \dots, k_{t-1})$$

$$\begin{aligned} \varphi_{\text{vigenere}}: \mathbb{Z}_{26} &\rightarrow \mathbb{Z}_{26} \\ x &\mapsto (x_i + k_{i \bmod t}) \bmod 26 \end{aligned}$$

message: ATTACKATDAWN
key: keykeykeykey
ciphertext: KXRKGIXBKAL

$$H_{\text{vigenere}} \simeq 4.7 \cdot t$$

Vernam cipher

$$k = (k_0, \dots, k_{n-1})$$

$$\begin{aligned}\varphi_{\text{vernam}}: \mathbb{Z}_{26} &\rightarrow \mathbb{Z}_{26} \\ x_i &\mapsto (x_i + k_i \bmod 26) \bmod 26\end{aligned}$$

message:	ATTACKATDAWN
key:	aezklwgrmali
ciphertext:	AXSKNGGKPOHV

$$H_{\text{vernam}} \simeq 4.7 \cdot n$$

If k is uniformly distributed and independent on m this cipher is perfect, i.e.

$$P[M = m | C = c] = P[M = m]$$

Nomenclators



Nomenclators

a b c d e f g h i k l m n o p q r s t u x y z
o ‡ ʌ # a □ θ ∞ i ð n // ø ∇ s m f Δ ε c 7 8 9

Nulles ff. — . — . d .

Dowbleth σ

and for with that if but where as of the from by

z 3 4 4 4 3 ʝ n m 8 x ∞

so not when there this in wich is what say me my wurt

ʝ x † ‡ 6 x 6 6 m n m m d

send lře receave bearer I pray you Mte your name myne

ʃ ſ ‡ T L H — ʒ 3 ss

Nomenclators

a b c d e f g h i k l m n o p q r s t u x y z
 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 10

Nulles ff. — . — . d .

Dowbleth 5

and for with that if but where as of the from by

2 3 4 4 4 3 7 11 13 15 17

so not when there this in wich is what say me my wyrt

[illegible]

send lre receive bearer I pray you Mte your name myne

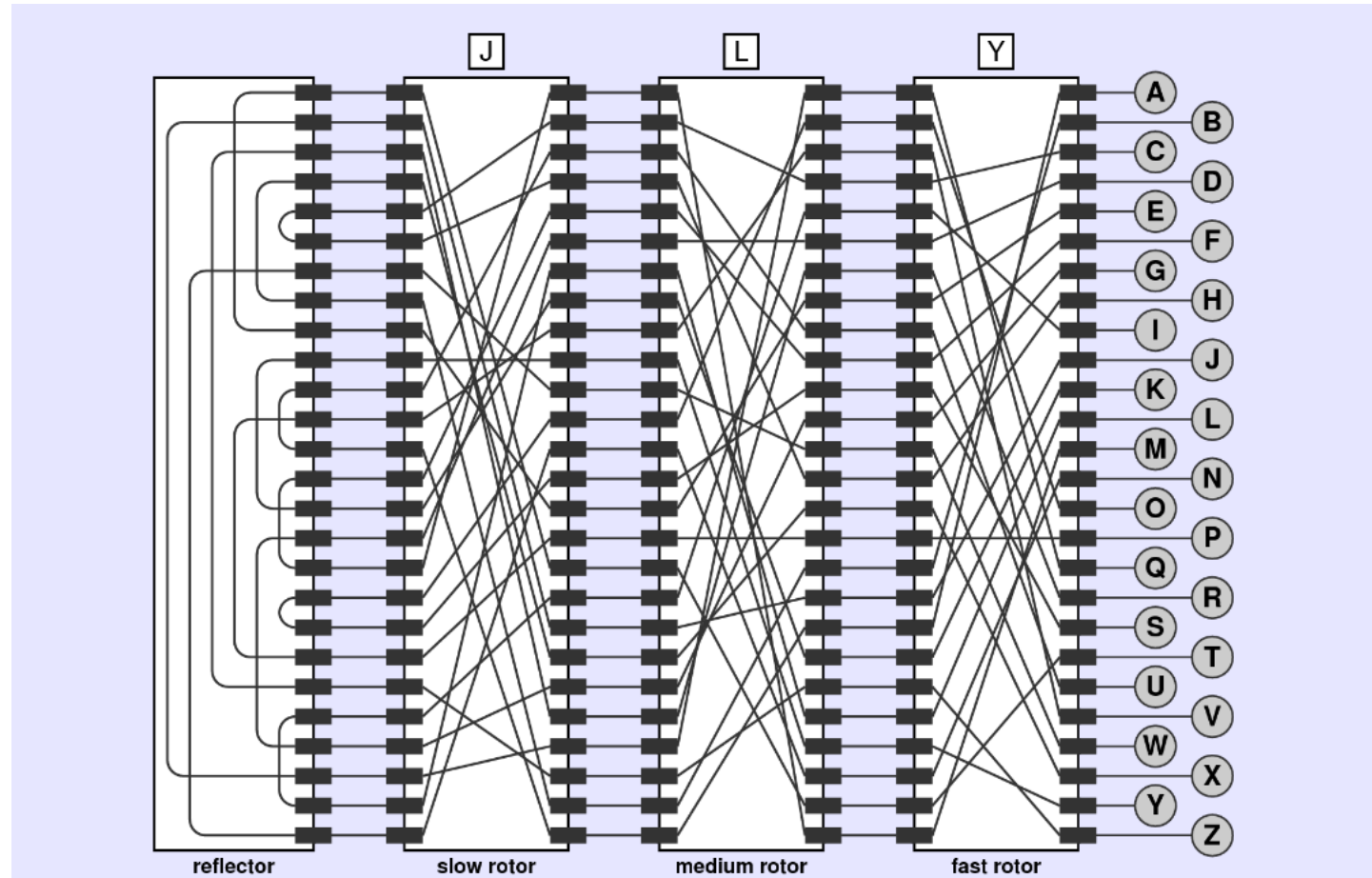
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 104



Machines to the rescue

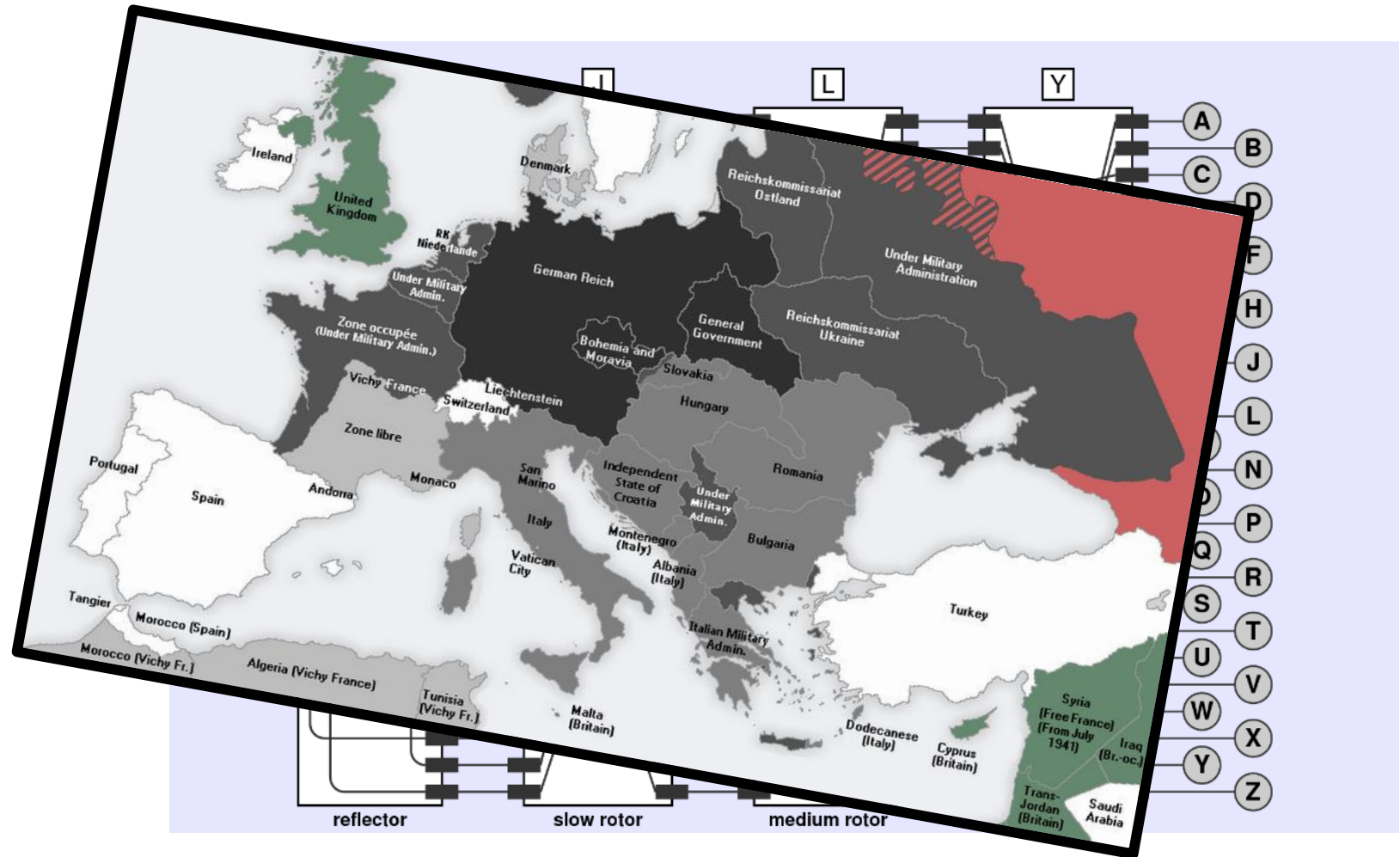


Machines to the rescue



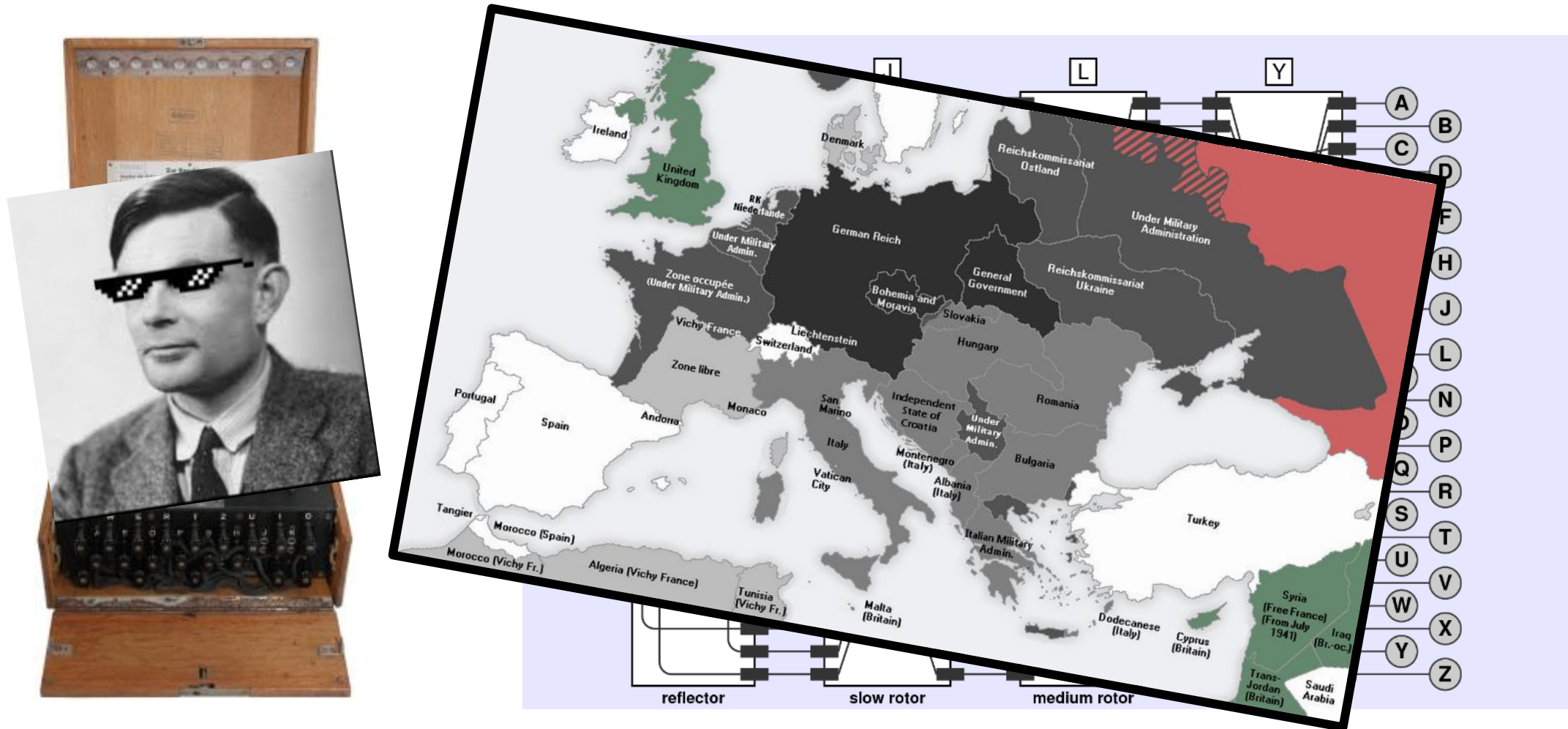
$$H_{enigma} = 65 \text{ or } 67$$

Machines “to the rescue”



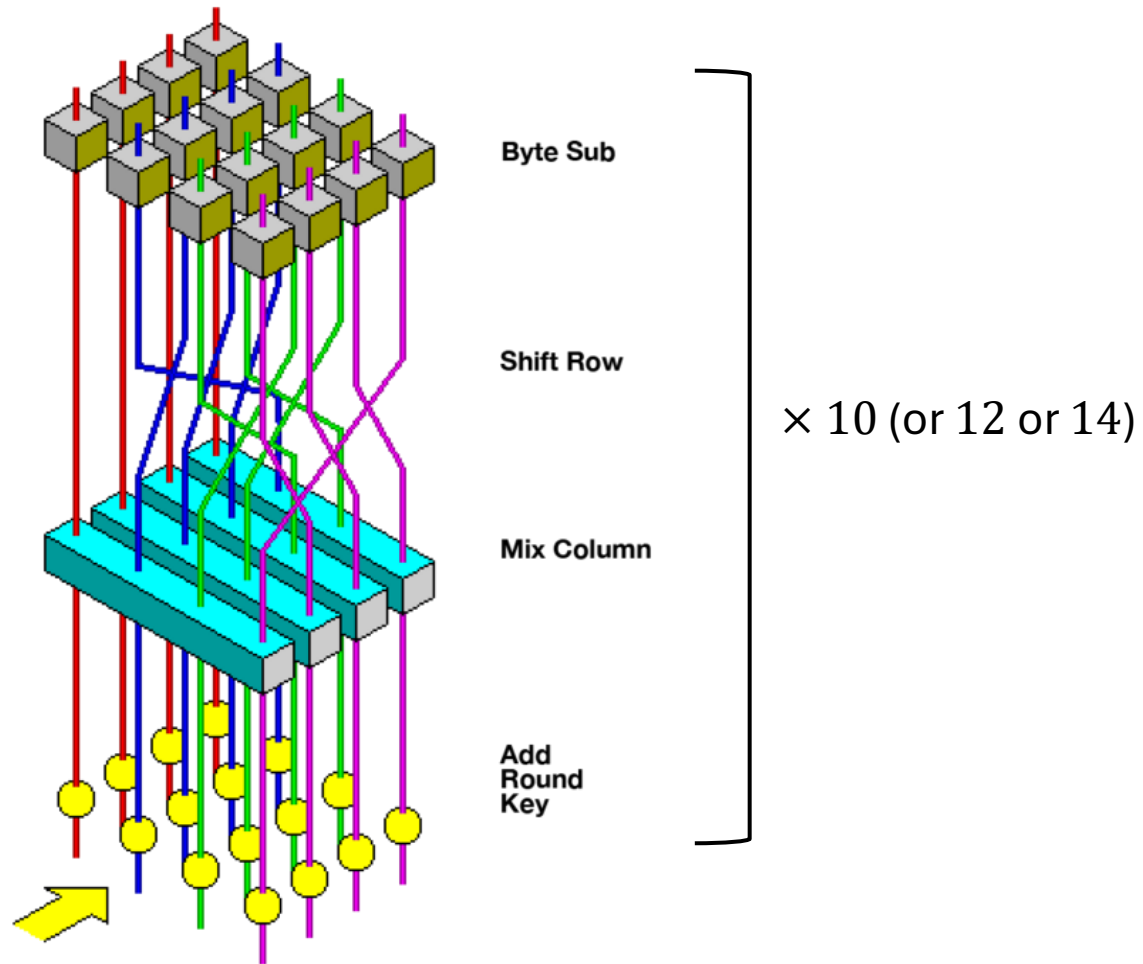
$$H_{\text{enigma}} = 65 \text{ or } 67$$

Machines “to the rescue”



$$H_{\text{enigma}} = 65 \text{ or } 67$$

Machines to the rescue



$$H_{AES} = 128 \text{ or } 192 \text{ or } 256$$

Machines to the rescue



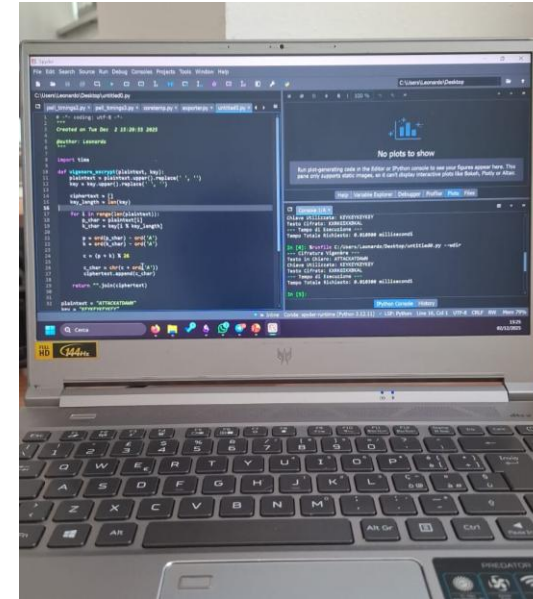
me

Vigenere

15 minutes (128 chars)

AES-128

6 to 8 hours (128 chars)



my laptop

0.00001 seconds

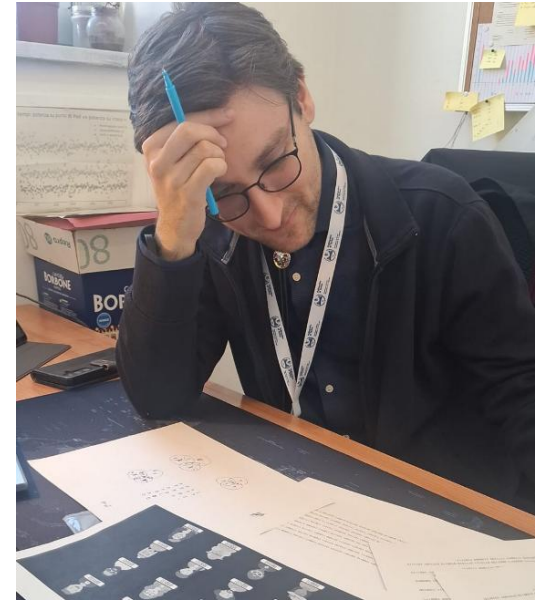
0.00015 seconds

** mathematicians were hurt for this demonstration*

Machines to the rescue



Encrypting (Dec. 2025)



Decoding (Feb. 2026)

The background is a solid dark blue. It features a faint, light blue illustration of a large, multi-story classical building with many windows and arches. Above the building, on the left, is a profile of a person wearing a classical helmet with a plume, holding a spear. There are also some leafy branches on the left and right sides. At the bottom center, the year '1850' is partially visible.

3: CODE-BASED CRYPTOGRAPHY

New paradigms

- Block ciphers
- Hash functions
- Stream ciphers
- Signature schemes
- Zero knowledge proofs
- Key encapsulation mechanisms
- ...



New paradigms

PRIVATE KEY

#

a very large
secret prime
number

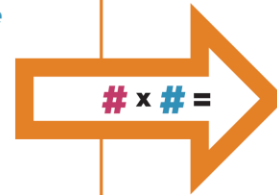
a very large
secret prime
number



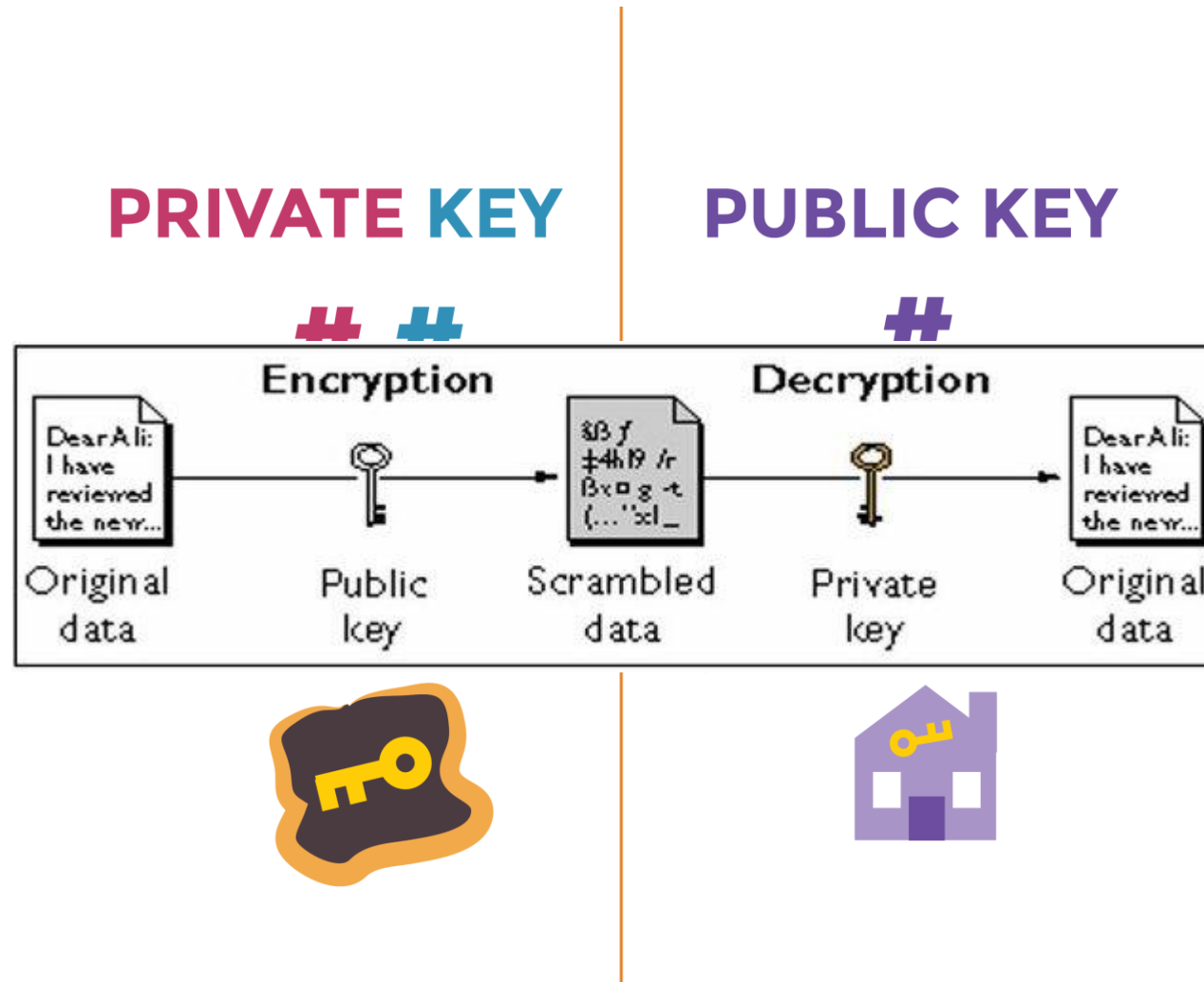
PUBLIC KEY

#

the product of those
two very large prime
numbers used to make
the private key, which
is very, very hard to
reverse back



New paradigms



McEliece (1978)

KeyGen:

G generator matrix of a code C

Δ efficient description of C decoding t errors

$G' = SG P$ for S change of basis, P permutation

public key G'

private key S, G, P

Encrypt(x):

$c \leftarrow xG$ encoding

$e \leftarrow$ random noise

return $y = c + e$

Decrypt(y)

return $x = \text{decode}(yP^{-1}, \Delta)S^{-1}$

** very very high-level*



Thanks!

1850