Information Theory
Thursday

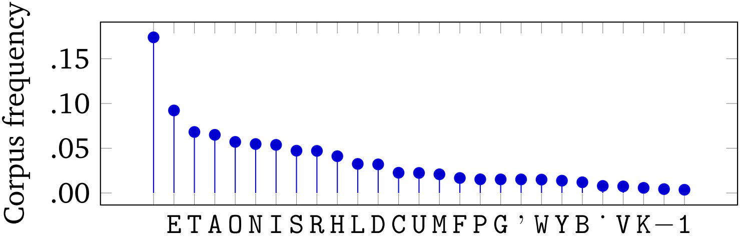
Mathias Winther Madsen
mathias@gmail.com
github.com/mathias-madsen/nasslli2025/

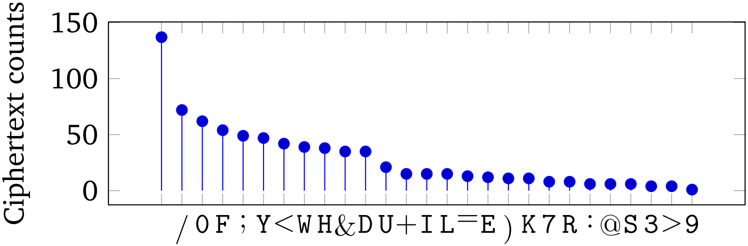
NASSLLI, June 2025

Substitution Ciphers

```
FLO DOOYW )YOS O;/ +OY;/YR O; F&/ U/)F &<;D EOH;E /<WFR F&/
UH;/ L<W KYO7/; K: F&/ /;FY: O) < +O=YF@ <;D 9=WF <F F&<F IO
H;FR < +/YF<H; WH;HWF/Y KUO+7 O) K=HUDH;E F&Y=WF )OYL<YD HFW
E<KU/ O; F&/ WFY//F3 HF L<W FLO WFOYH/W &HE&@ W&OL/D ;O LH;
DOLR ;OF&H;E K=F < DOOY O; F&/ UOL/Y WFOY: <;D < KUH;D )OY/&
/<D O) DHW+OUO=Y/D L<UU O; F&/ =II/Y@ <;D KOY/ H; />/Y: )/<F
=Y/R F&/ S<Y7W O) IYOUO;E/D <;D WOYDHD ;/EUHE/;+/3 F&/ DOOYR
L&H+& L<W /M=HII/D LHF& ;/HF&/Y K/UU ;OY 7;O+7/YR L<W KUHWF
/Y/D <;D DHWF<H;/D3 FY<SIW WUO=+&/D H;FO F&/ Y/+/WW <;D WFY=
+7 S<F+&/W O; F&/ I<;/UW@ +&HUDY/; 7/IF W&OI =IO; F&/ WF/IW@
F&/ W+&OOUKO:  &<D FYH/D &HW 7;H)/ O; F&/ SO=UDH;EW@ <;D )OY
+UOW/ O; < E/;/Y<FHO;R ;O O;/ &<D <II/<Y/D FO DYH>/ <L<:  F&
/W/ Y<;DOS >HWHFOYW OY FO Y/I<HY F&/HY Y<><E/W3
```

Substitution Ciphers

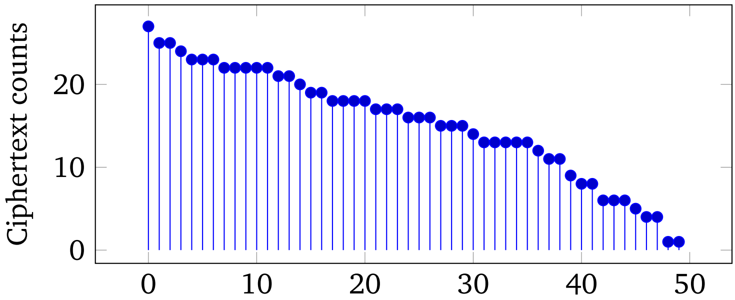




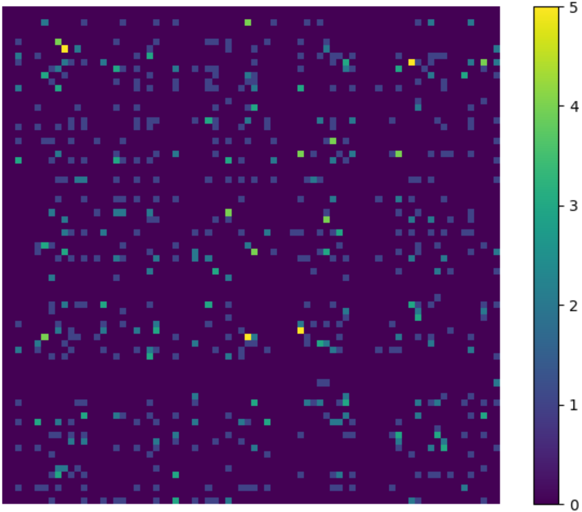
One-to-Many Substitution Ciphers

_	63, 17, 52, 7, 18, 34, 73
E	75, 9, 38, 11
T	50, 2, 36
A	5, 29, 48
O	71, 65, 22
N	8, 45
I	49, 12
S	23, 20
R	26, 60
⋮	⋮

One-to-Many Substitution Ciphers



One-to-Many Substitution Ciphers



One-to-Many Substitution Ciphers

Ravi and Knight: “Bayesian inference for Zodiac and other homophonic ciphers,” *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics*, 2011.

Permutation Ciphers

```
FOR _TH E_N EXT _FO UR_ DAY S_I T_S EEM ED_ ...
```

$$\updownarrow$$

```
ORF TH_ _NE XTE FO_ R_U AYD _IS _ST EME D_E ...
```

Permutation Ciphers

From bigrams alone:

HEEWR	:	WHERE (49.3%)	EWHER (10.9%)	REWHE (8.6%)	HEREW (6.0%)
TTAH	:	THAT (55.8%)	TATH (16.1%)	ATHT (9.6%)	TTHA (6.8%)
TINGH	:	THING (45.2%)	TINGH (11.8%)	NGITH (8.0%)	NGHIT (7.6%)
OECN	:	ECON (20.3%)	CONE (18.1%)	ENCO (17.5%)	ONCE (16.8%)
DSAI	:	ADIS (22.4%)	DISA (9.9%)	ASID (9.9%)	ISAD (9.7%)

Periodic Substitution Ciphers

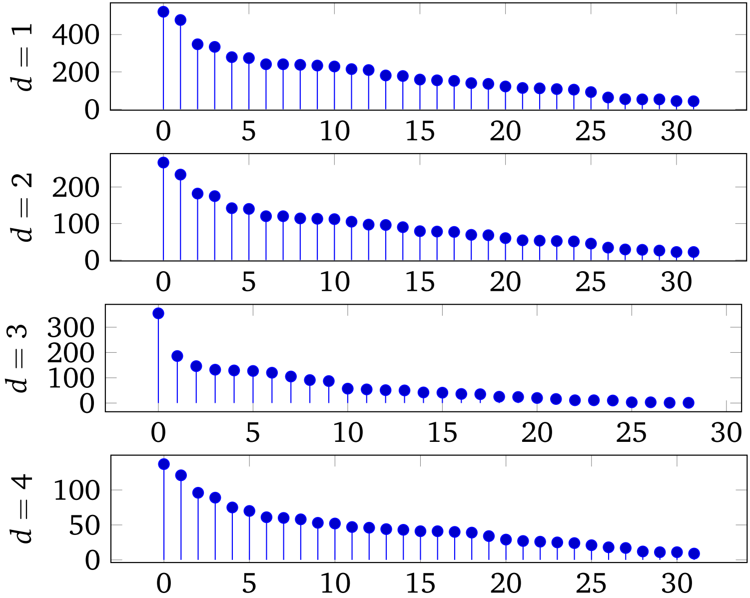
	$1, 4, 7, \ldots$	$2, 5, 8, \ldots$	$3, 6, 9, \ldots$
A	C	B	A
B	A	C	B
C	B	A	C

ABB BCA CCB AAB BCA . . .

$$\updownarrow$$

CCB AAA BAB CBB AAA . . .

Periodic Substitution Ciphers



Periodic Substitution Ciphers

An Enigma machine

Periodic Substitution Ciphers

Henryk Zygalski, Jerzy Różycki, and Marian Rejewski in Poznań
(photo by Adam Mickiewicz, 1932)

Rejewski: "How Polish Mathematicians Deciphered the Enigma," *IEEE Annals of the History of Computing*, 1981.

Perfect Secrecy

Definition

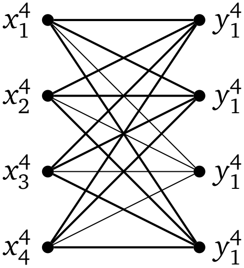
An encoding method achieves **perfect secrecy** if

$$p(x^n \mid y^n) = p(x^n)$$

for all plaintext messages x^n and ciphertexts y^n.

Shannon: "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, 1949.

Perfect Secrecy



	Message			
Key	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

Theorem: Size of the Keyspace

A perfectly secret code has at least as many keys as there are (nonzero-probability) plaintext messages.

One-Time Pad

x^n	A	B	A	A	B	A	A	$\cdots$	B
k^n	0	1	1	0	0	1	1	$\cdots$	0
y^n	A	A	B	A	B	A	A	$\cdots$	B

Running-Key Ciphers

x^n	T	H	E	_	G	R	E	$\cdots$	.
k^n	W	H	E	N	_	S	H	$\cdots$	.
y^n	P	5	/	N	G	J	2	$\cdots$	<

Marginal, Conditional, and Joint Entropy

Definition

$$H(X) = E\left(\log_2 \frac{1}{p(X)}\right)$$

$$H(X \mid Y) = E\left(\log_2 \frac{1}{p(X \mid Y)}\right)$$

$$H(X, Y) = E\left(\log_2 \frac{1}{p(X, Y)}\right)$$

Theorem

$$H(X, Y) \ = \ H(X \mid Y) + H(Y)$$

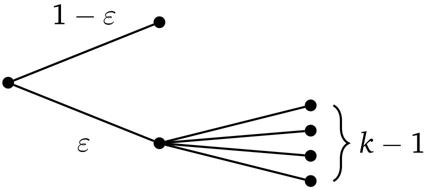
Theorem

$$H(X \mid Y) \ \leq \ H(X)$$

Fano's Inequality

Theorem: Fano's Inequality

Let X be a random variable that can take k different values, one of which has probability $1-\varepsilon$. Then $H(X) \leq 1 + \varepsilon \log_2 k$.



In fact

$$\varepsilon H_2(1/k) \;\leq\; H(X) \;\leq\; 1 + \varepsilon \log_2 k,$$

or equivalently,

$$\frac{H(X)-1}{\log k} \;\leq\; \varepsilon \;\leq\; \frac{H(X)}{H_2(1/k)}.$$

Entropy for Codebreaking

$$H(X^n \mid Y^n) \;\leq\; H(X^n, K \mid Y^n) \;=\; H(K \mid Y^n) \;\leq\; H(K)$$