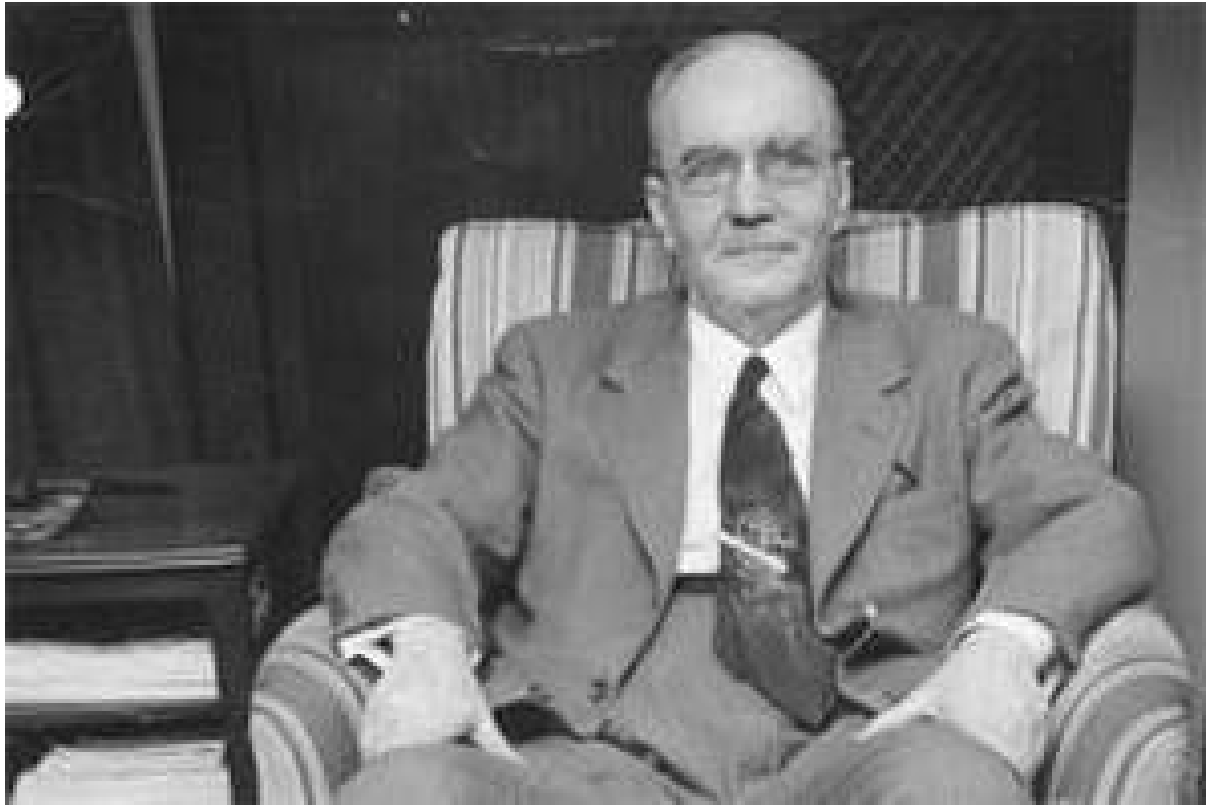
The Hill Cipher

Frank Rubin

Lester S. Hill



Invented by Lester S. Hill of Hunter College, Brooklyn.

Published in American Mathematical Monthly, June 1929.

Similar cipher invented by Jack Levine of North Carolina State College in 1924.

Published in Flynn's Weekly, a pulp detective magazine in Oct. 1926.

(Hill was 38, Levine was 17.)

OUTLINE

Mathematical era

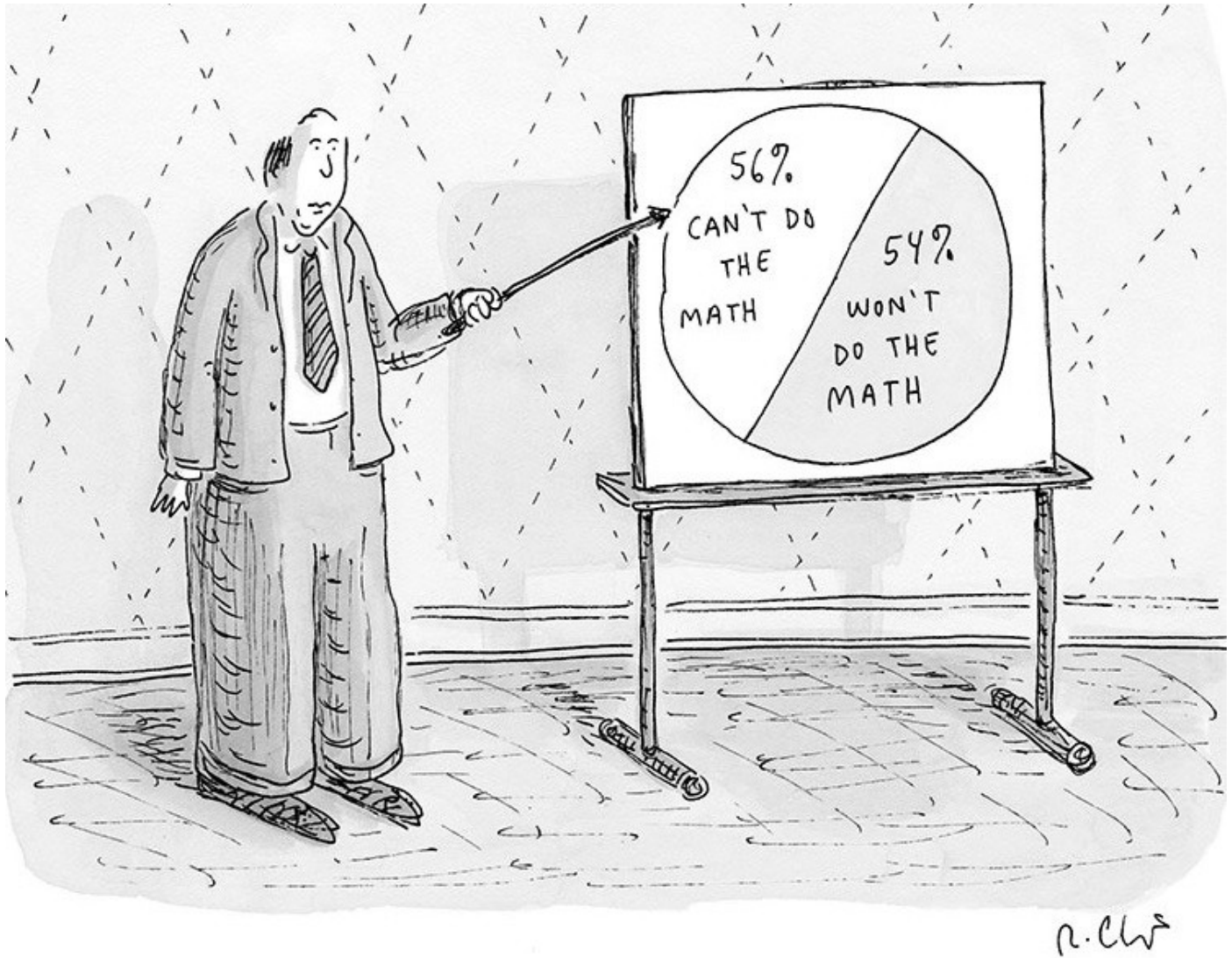
* How it works

* How to defeat it

* How to prevent that

* How to make it fast

Unbreakable


56%
CAN'T DO THE MATH
54%
WON'T DO THE MATH

Standard English Alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Runs from 0 to 25.

Mixed Alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M
4	21	0	13	18	6	10	23	15	3	19	7	11

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
16	5	25	8	20	1	12	24	2	22	14	9	17

Runs from 0 to 25.

Matrix Method

P = Plaintext, the message to be enciphered
C = Ciphertext, the enciphered message
Matrix encryption C = AP + B

$$\underset{\text{C}}{\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix}} = \underset{\text{A}}{\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}} \underset{\text{P}}{\begin{pmatrix} P1 \\ P2 \\ P3 \end{pmatrix}} + \underset{\text{B}}{\begin{pmatrix} j \\ k \\ l \end{pmatrix}}$$

C1 = (aP1 + bP2 + cP3 + j) mod 26
C2 = (dP1 + eP2 + fP3 + k) mod 26
C3 = (gP1 + hP2 + iP3 + l) mod 26

Decipher

$C = AP + B$

$C-B = AP$

$A'(C-B) = P$

$P = A'(C-B)$

A' is the inverse of A, so $A'A = AA' = I$, where I is the identity matrix.

Simple Case, Standard Alphabet, B=0

Probable word, word dragging.

BNCSVTJIQPLXEWH

∘∘∘ARTILLERY∘∘∘

Set up linear equations

$a\mathbf{A} + b\mathbf{R} + c\mathbf{T} = \mathbf{S} \bmod 26$

$d\mathbf{A} + e\mathbf{R} + f\mathbf{T} = \mathbf{V} \bmod 26$

$g\mathbf{A} + h\mathbf{R} + i\mathbf{T} = \mathbf{T} \bmod 26$

$a\mathbf{I} + b\mathbf{L} + c\mathbf{L} = \mathbf{J} \bmod 26$, etc.

Semi-Simple, Standard Alphabet, B≠0

Probable word, word dragging.

BNCSVTJIQPLXEWHPOUWL

∘∘∘**ARTILLERYRANGE**∘∘∘

Set up linear equations

a**A** + b**R** + c**T** + j = **S** mod 26

d**A** + e**R** + f**T** + k = **V** mod 26

g**A** + h**R** + i**T** + l = **T** mod 26

a**I** + b**L** + c**L** + j = **J** mod 26, etc.

Bigrams and Trigrams, Oh My!

Pairs of letters are called *bigrams*, triples are called *trigrams*.

Simple substitution ciphers are solved by using letter frequency and letter contact frequency.

The same can be done with bigrams, trigrams, etc.

In the general case, mixed alphabets, $B \neq 0$, forget about the linear relationship and solve as trigram substitution.

Separability

In each block, notice that the first letter depends only on the top row of the matrix, the second letter depends only on the second row, etc.

You can brute-force each row. Try all 26^3 or 26^4 possibilites, and test which gives the best letter frequencies.

Low-frequency letters are most important. It's not so much getting lots of E, T, A but fewest J, Q, Z. Take the best row candidates and try pairs.

This attack can be defeated by using a mixed alphabet.

2-Sided Multiplication

Separability can be defeated by multiplying by matrices on both sides. There are two linear steps.

$X = AP + B$

$C = X^{\mathsf{T}}D + E$

P = original plaintext

X = intermediate ciphertext (column vector)

X^{T} = X transpose (rows↔columns)

C = final ciphertext (row vector)

Even if we set D=A, that is, we multiply P on both sides by the original matrix A, every ciphertext character is still a linear combination of the 3 plaintext characters, but the coefficients are now quadratic in *a*, *b*, *c*, …

With B=0, there will be 27 of the 81 possible quadratic terms. With B≠0, there will be 36 out of 108 possible quadratic terms, plus 3 linear terms.

Either way, exhaustive trial of $26^{12} = 9.54 \times 10^{16}$ possible values is barely feasible, and solving 12 quadratic equations in 12 unknowns would be seriously challenging.

So even the 3×3 case is fairly secure.

Modern Version

In the modern version, 8-bit bytes replace the 26-letter alphabet. Matrix operations are modulo 256.

It is not feasible to have crypto clerks in the field generate invertible matrices and then invert them. So, leave the matrices fixed and vary the substitutions. Here is one idea:

1) Simple substitution S.
2) Left multiply by matrix A.
3) Simple substitution T.
4) Right multiply by matrix B.
5) Simple substitution U.

General Ring

A ring is a set of elements that behave like integers under addition and multiplication.

$a+b$ and ab are elements of the ring.

$a+(b+c)=(a+b)+c$.

$a+b=b+a$.

There is a ring element 0 such that $0+a=a+0=a$.

There is an element $-a$ such that $a+(-a)=(-a)+a=0$.

$a(bc)=(ab)c$.

$a(b+c)=ab+ac$, and $(a+b)c=ac+bc$.

There is a ring element 1 such that $1a=a1=a$.

Gaussian Integers

One possible 256-element ring is the Gaussian integers, or complex integers, numbers of the form X+Yi. Here i is the imaginary square root of -1, and X and Y are hex digits, that is, integers modulo 16. All arithmetic is modulo 16.

$$(A+Bi) + (C+Di) = (A+C) + (B+D)i,$$
$$(A+Bi) \times (C+Di) = (AC-BD) + (AD+BC)i$$

Quaternions

Invented by Irish mathematician William Rowan Hamilton to represent the motions of a spinning object.

Numbers of the form W+Xi+Yj+Zk, where W, X, Y and Z are integers, and i, j and k are abstract elements obeying the rules ij=k, jk=i, ki=j, and ji=-k, kj=-i and ik=-j.

All arithmetic is modulo 4.

$$(A+Bi+Cj+Dk) + (E+Fi+Gj+Hk) =$$
$$(A+E) + (B+F)i + (C+G)j + (D+H)k,$$
$$(A+Bi+Cj+Dk) \times (E+Fi+Gj+Hk) =$$
$$(AE-BF-CG-DH) + (AF+BE+CH-DG)i +$$
$$(AG-BH+CE+ DF)j + (AH+BG-CF+DE)k.$$

Combining these Ideas

Two-sided multiplication

1) Simple substitution S – bytes.
2) Left multiply by matrix A – Gaussian integers.
3) Simple substitution T – bytes.
4) Right multiply by matrix B – Quaternions.
5) Simple substitution U – bytes.

10×10 matrices is sufficient. This takes 20 ring multiplications and 18 additions per character.

Make it Faster

Fixed-size blocks, everything aligns.

```
AAAbbbCCCdddEEEfff
PPPqqqRRRsssTTTuuu
```

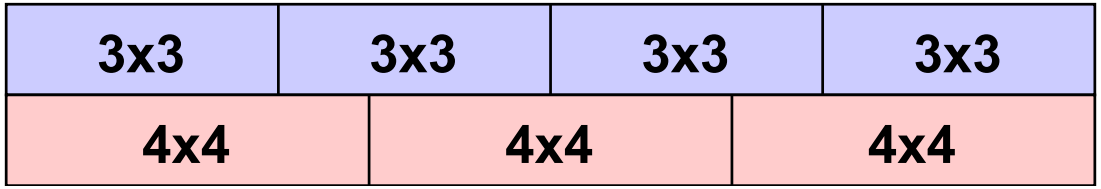
Variable-sized blocks, accidental alignment.

```
AAAbbbbCCCddddddEEEE
PPPPqqqRRRsssTTTuuuu
```

Still need 10×10 or larger matrices.

Offset

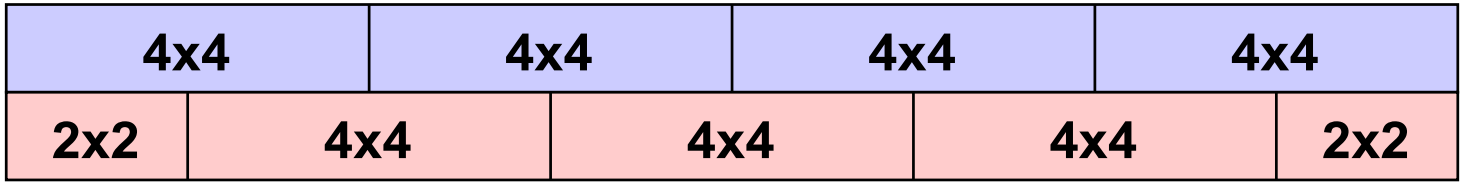
Use fixed-sized blocks, offset so every ciphertext character depends on plaintext characters from 2 different blocks.



The effective block size is 12 characters. If the matrix sizes are N×N and M×M, the effective block size is lcm(N,M).

Brick Wall

Use same-sized blocks, offset so block boundries never align.
The ciphertext block is the entire message.



Conclusion

Two rounds of the Hill cipher can produce a cipher which is both very fast and very secure.