SUBSTITUTION CODES

MTH 440

Direct Numerical Substitution

L	#		L	#
A	0		N	13
B	1		O	14
C	2		P	15
D	3		Q	16
E	4		R	17
F	5		S	18
G	6		T	19
H	7		U	20
I	8		V	21
J	9		W	22
K	10		X	23
L	11		Y	24
M	12		Z	25

THIS IS EASY
19 7 8 18 8 18 4 9 18 24

Caesar Shift

- Substitution cipher where all letters are shifted by 3

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

I am weak.

L dp zhdn.

Decipher: MXOLXV

Simple substitution

We don’t have to shift by 3, we can shift by any amount. How many guesses would you need to get his one?
Assume spacing is preserved.

Q ewctl tqsm bw wzlmz i xqhhi.

(http://rumkin.com/tools/cipher/caesar.php)

L	#		L	#
A	0		N	13
B	1		O	14
C	2		P	15
D	3		Q	16
E	4		R	17
F	5		S	18
G	6		T	19
H	7		U	20
I	8		V	21
J	9		W	22
K	10		X	23
L	11		Y	24
M	12		Z	25

Add a codeword then shift by 3

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

Is this better?
Nk lrnk yellej?

http://rumkin.com/tools/cipher/caesar-keyed.php
http://rumkin.com/tools/cipher/cryptogram-solver.php

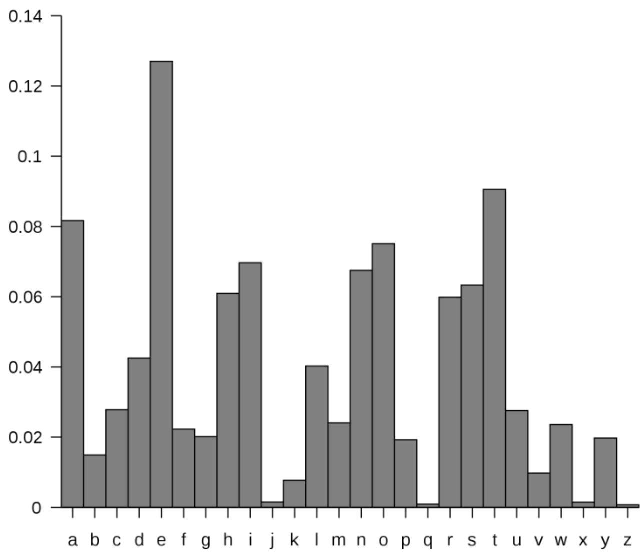
Better yet (?) permute randomly

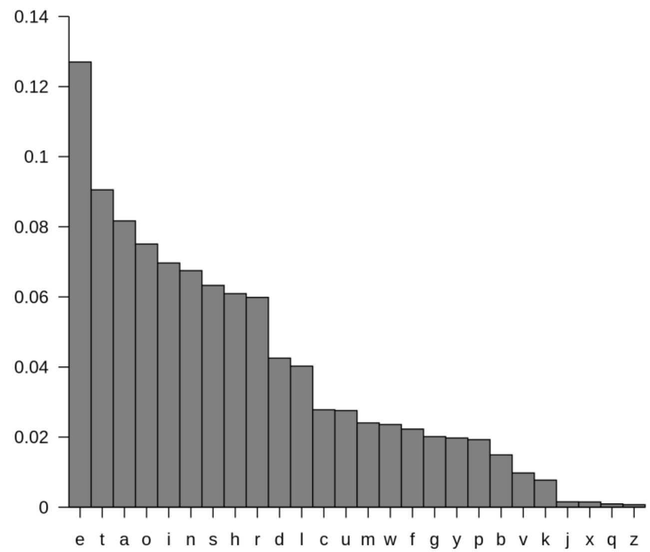
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	?
?	?	?																							

R X L H V E   V X H N V E   K X H V D   P X H N   X H D

H V V H N   A E   B C D N V D   R X H N   X H D   H C X B

(FREQUENCY, HELPFUL, CRIB)





Let's switch to numbers…

L	#		L	#
A	0		N	13
B	1		O	14
C	2		P	15
D	3		Q	16
E	4		R	17
F	5		S	18
G	6		T	19
H	7		U	20
I	8		V	21
J	9		W	22
K	10		X	23
L	11		Y	24
M	12		Z	25

We can think of "shifting by 3" as "adding 3" remembering that if the number is greater than 25 we loop back around to the beginning.

Shift by 3:

$E \to 4 \to 4 + 3 = 7 \to H$
$Y \to 24 \to 24 + 3 = 27 - 26 = 1 \to B$

This is arithmetic modulo 26 (if a number is greater than 26, we instead replace it by the remainder upon division by 26).

Shift Cipher, Shift = key

- To encipher

$$PT \rightarrow CT: CT = PT + K \pmod{26}$$

- To decipher

$$CT \rightarrow PT: PT = CT - K \pmod{26}$$

- Clearly to break we only need to check 25 “keys”

Decimation Cipher

- What if we multiplied instead of added?
- To encipher

$$CT = PT * K \pmod{26}$$

Example

Let k = 5

$L \rightarrow 11 \rightarrow 11 * 5 \pmod{26} = 55 \pmod{26} = 3 \rightarrow D$

How do you decipher?

Look up table

- If you had a table of how to encipher all letters you could just use it in reverse to decipher

D	E	C	I	M	A	T	I	O	N		F	O	R		K	=	5								
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
A	F	K	P	U	Z	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V

- Decipher: GUDDPSNU
- You try – see handout

Modular Facts

a is the "inverse" of b modulo n if

ab = ba = 1 (mod n)

Fact: Given n and a such that 0<a<n, then a has an inverse modulo n if and only if gcd(a,n) = 1.

How do you find an inverse?

1) If you have a multiplicative Cayley table, you could just examine the table for the inverse. Use your Cayley table to find the inverse of 21 modulo 26.
2) Guess and check: Find the inverse of 5 modulo 11.
3) Extended Euclidean Algorithm (take number or group theory)

Decimation Ciphers: a*PT (mod 26)

- You will only be able to decipher to a unique ciphertext if a has an inverse modulo 26.

- A will always be enciphered to A.
- Assuming a key with an inverse was used, how many guesses would you have to make to find the key?
- Using a frequency analysis we could just guess one letter and then check to see if it worked.

Affine Ciphers: a*PT + b (mod 26)

- Assuming we only use a’s with inverses, how many different keys would an attacker have to guess?
- A frequency analysis can still help, but we have two variables to solve for so we need two equations.
- Suppose we were given the following ciphertext that we know was enciphered using an affine cipher:

```
Hv ufe fh kar karvedrh vu pfkarpfkdlh fer
fivnk erfmdkz, karz fer svk lrekfds; hv ufe
fh karz fer lrekfds, karz fer svk fivnk
erfmdkz. – Fmirek Rdshkrds.
```

Frequency Analysis/Finding a & b

Hv ufe fh kar karvedrh vu pfkarpfkdlh fer fivnk erfmdkz, karz fer svk lrekfds; hv ufe fh karz fer lrekfds, karz fer svk fivnk erfmdkz. – Fmirek Rdshkrds

Letter	Count
R	18
F	17
K	17
E	12
D	8
V	8

Most common English letters: e,t,a,o,i,n,s

Guess & Check

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

http://rumkin.com/tools/cipher/frequency.php (freq. analysis)

http://rumkin.com/tools/cipher/affine.php (affine checker)