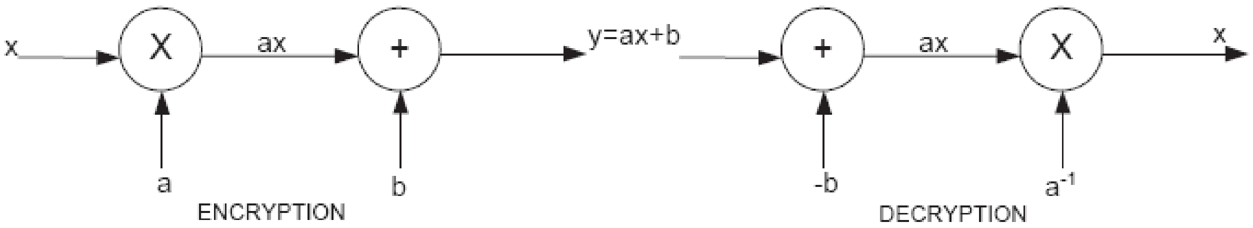
Fundamentals of Information & Network Security ECE 471/571

Lecture #5: Early Ciphers
Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Affine Cipher

- Affine transformation: scale and then shift

$$y = e_K(x) = (ax + b) \mod 26,$$
$$d_K(y) = a^{-1}(y - b) \mod 26.$$



- An example of an affine cipher: a=9, b=3

- Problem with choice of a?

- *Multiplicative inverse*: if x × y = 1 mod n, then x and y are each other's multiplicative inverse mode n
  - Example: 3 × 7 = 1 mod 10

The Cardinality of Key Space for the Affine Cipher

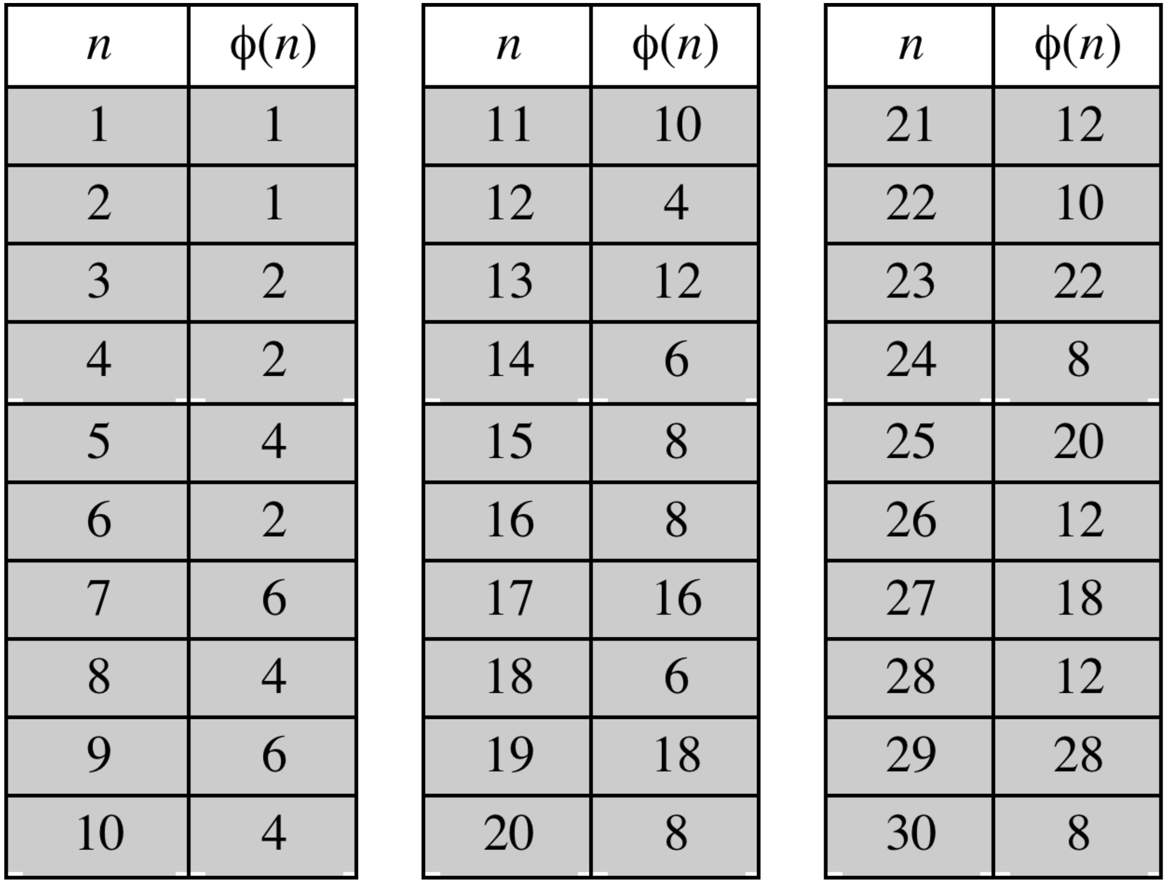
- a has multiplicative inverse mod n iff a is relatively prime to n, or gcd(a,n) = 1

- How many of them? --- $\phi(n)$: Euler totient function
  - number of integers less than n and relatively prime to n.
  - $\phi(n) = n - 1$ if n is prime
  - $\phi(p \times q) = (p - 1)(q - 1)$ if p and q are prime
  - In general……

- The number of possible keys in Affine Cipher is $n \times \phi(n)$

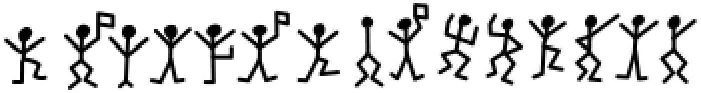
Euler’s Totient Function *ø(n)*

- Number of positive integers less than n and relatively prime to n.
- If n=p*q, where p and q are primes, then *ø(n)=(p-1)(q-1)*



n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

(This table can be found on page 48 in the textbook)



Substitution Cipher

- The key can be any permutation of the 26 alphabetic characters

$$
\begin{aligned}
y = e_\pi(x) &= \pi(x), \\
d_\pi(y) &= \pi^{-1}(y).
\end{aligned}
$$

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

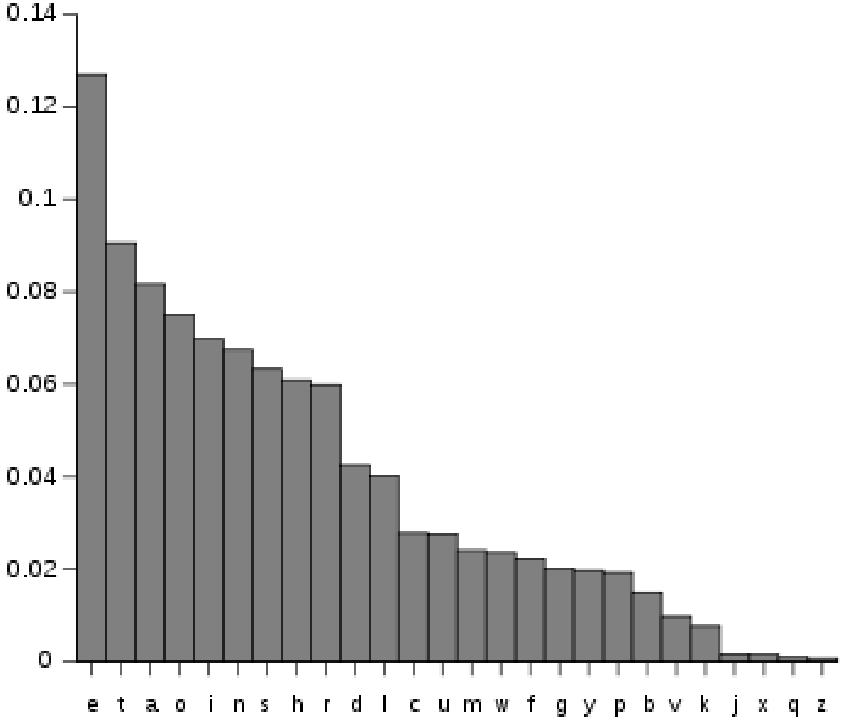
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

Substitution -> VUNVMZMUMZFS

- Question: How many possible keys? Is it secure enough?

Frequency Analysis

- Exploit the regularities of the language and counting letter frequencies
  - Similarly we can define, frequencies of digrams, trigrams, initial letters, final letters, etc.



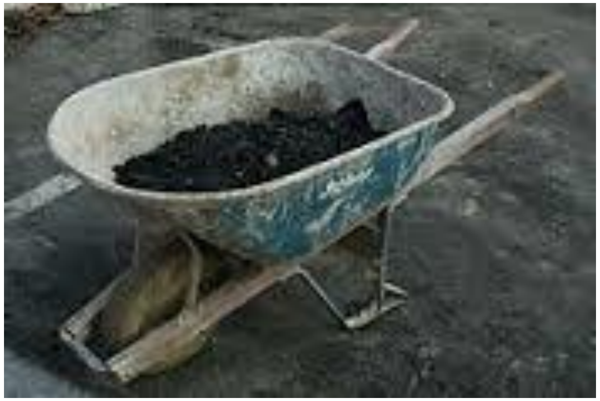
Question: which one is easier to break, a longer ciphertext or a shorter one?

Activity

Let’s crack this substitution cipher (see handouts):

EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCKQPKUGK
MGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCGOIDPKZCNKSHICGI
WYGKKGKGOLDSILKGOIUSIGLEDSPWZUGFZCCNDGYYSFUSZCNXEOJNC
GYEOWEUPXEZGACGNFGLKNSACIGOIYCKXCJUCIUZCFZCCNDGYYSFEU
EKUZCSOCFZCCNCIACZEJNCSHFZEJZEGMXCYHCJUMGKUCY

https://cryptoclub.org/#vAllTools



wheelbarrow