Introduction to Cryptography: Alphabet Codes

Introduction to Cryptography: Alphabet Codes: Steven J. Miller

http://www.williams.edu/Mathematics/sjmiller/public_html

VCTAL: Burlington, June 19, 2019

Caesar and Affine Ciphers

Encryption Functions

Function from alphabet to alphabet such that:

- Different letters go to different letters.
- All letters hit.

Do we need both conditions?

Encryption Functions

Function from alphabet to alphabet such that:

- Different letters go to different letters.
- All letters hit.

Do we need both conditions?
Setup: x input letter, $f(x)$ is the encrypted letter.

Caesar Cipher

Cannot use $f(x) = c$ for a constant c: Why?
Next simplest function is $f(x) = x + c$ for some constant.

Caesar Cipher

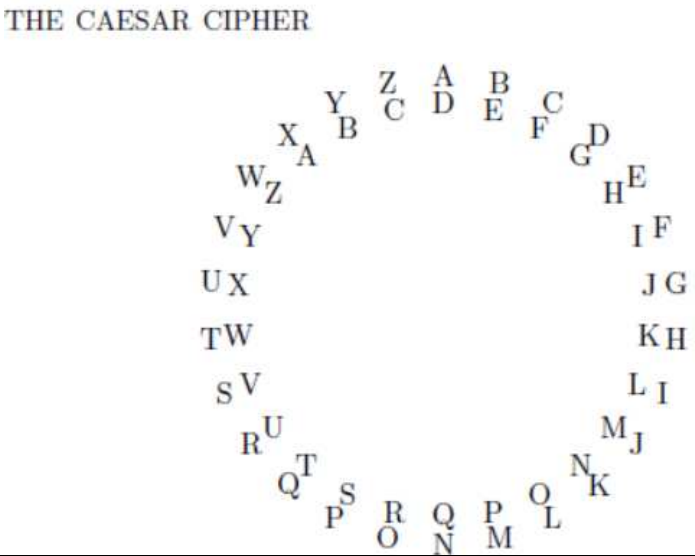
Cannot use $f(x) = c$ for a constant c: Why?
Next simplest function is $f(x) = x + c$ for some constant.

- $c = 3$ is the standard Caesar cipher: how many choices?
- $A \to D, B \to E, \ldots, W \to Z, X \to A, Y \to B, Z \to C$ (clock arithmetic).
- How do we decrypt?

Caesar Cipher: Illustration

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

Caesar Cipher: Illustration



Caesar Cipher: Example

	M	E	E	T	A	T	T	E	N
	12	4	4	19	0	19	19	4	13
add 3:	15	7	7	22	3	22	22	7	16
	P	H	H	W	D	W	W	H	Q

	P	H	H	W	D	W	W	H	Q
	15	7	7	22	3	22	22	7	16
subtract 3:	12	4	4	19	0	19	19	4	13
	M	E	E	T	A	T	T	E	N

Affine Cipher: $f(x) = ax + b$

Try more complicated function: $f(x) = ax + b$.

What b are possible?

Often best to start simple: take 6 letter alphabet: $\{A, B, C, D, E, F\}$.

To do calculations let $A = 1$, $B = 2$, $\ldots$, $F = 6$.

Do all b work? Do all a work?

Affine Cipher: II: $f(x) = ax + b$

Have $A = 1, B = 2, \dots, F = 6$, look modulo 6.

Enough to study a and take $b = 0$: $f(x) = ax$.

Affine Cipher: II: $f(x) = ax + b$

Have $A = 1, B = 2, \ldots, F = 6$, look modulo 6.

Enough to study a and take $b = 0$: $f(x) = ax$.

$$\begin{array}{ccccccccccc} A & +1 \Rightarrow & B & +1 \Rightarrow & C & +1 \Rightarrow & D & +1 \Rightarrow & E & +1 \Rightarrow & F \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ C & +1 \Rightarrow & D & +1 \Rightarrow & E & +1 \Rightarrow & F & +1 \Rightarrow & A & +1 \Rightarrow & B \end{array}$$

$$\begin{array}{ccccccccccc} A & +1 \Rightarrow & B & +1 \Rightarrow & C & +1 \Rightarrow & D & +1 \Rightarrow & E & +1 \Rightarrow & F \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ C & +2 \Rightarrow & E & +2 \Rightarrow & A & +2 \Rightarrow & C & +2 \Rightarrow & E & +2 \Rightarrow & A \end{array}$$

Affine Cipher: II: $f(x) = ax + b$

Have $A = 1, B = 2, \ldots, F = 6$, look modulo 6.

Enough to study a and take $b = 0$: $f(x) = ax$.

- $a = 1$: works: get $\{1, 2, 3, 4, 5, 6\}$.
- $a = 2$: fails: get $\{2, 4, 6, 2, 4, 6\}$ (thus 4 and 6 will also fail).
- $a = 3$: fails: get $\{3, 6, 3, 6, 3, 6\}$ (and also get again 6 fails).
- $a = 5$: works: get $\{5, 4, 3, 2, 1, 6\}$.

Affine Cipher: II: $f(x) = ax + b$

Have $A = 1, B = 2, \ldots, F = 6$, look modulo 6.

Enough to study a and take $b = 0$: $f(x) = ax$.

- $a = 1$: works: get $\{1, 2, 3, 4, 5, 6\}$.
- $a = 2$: fails: get $\{2, 4, 6, 2, 4, 6\}$ (thus 4 and 6 will also fail).
- $a = 3$: fails: get $\{3, 6, 3, 6, 3, 6\}$ (and also get again 6 fails).
- $a = 5$: works: get $\{5, 4, 3, 2, 1, 6\}$.

1, 5 work and 2, 3, 4, 6 fail: What's the pattern?

Affine Cipher: III: $f(x) = ax + b$

Alphabet is $A = 1, \ldots, F = 6$.

The a that work are relatively prime to 6....

What do you think works for 26 letter alphabet?

Affine Cipher: III: $f(x) = ax + b$

Alphabet is $A = 1, \ldots, F = 6$.

The a that work are relatively prime to 6....

What do you think works for 26 letter alphabet?

Answer: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25: 12 choices.

Caesar cipher: 26 choices; Affine cipher: $12 \cdot 26 = 312$.

Can we go to higher degree polynomials?

Totient Function

Will use the Euler totient function $\phi(n)$ later.
$\phi(n)$ is the number of numbers from 1 to n that are relatively prime to n.

If p prime, $\phi(p) =$

Totient Function

Will use the Euler totient function $\phi(n)$ later.
$\phi(n)$ is the number of numbers from 1 to n that are relatively prime to n.

If p prime, $\phi(p) = p - 1$.

If $n = p^2$, $\phi(p^2) =$

Totient Function

Will use the Euler totient function $\phi(n)$ later.
$\phi(n)$ is the number of numbers from 1 to n that are relatively prime to n.

If p prime, $\phi(p) = p - 1$.

If $n = p^2$, $\phi(p^2) = p^2 - p$ (lose $p, 2p, 3p, \ldots, p^2$.

If $n = p^3$, $\phi(p^3) =$

Totient Function

Will use the Euler totient function $\phi(n)$ later.
$\phi(n)$ is the number of numbers from 1 to n that are relatively prime to n.

If p prime, $\phi(p) = p - 1$.

If $n = p^2$, $\phi(p^2) = p^2 - p$ (lose $p, 2p, 3p, \ldots, p^2$.

If $n = p^3$, $\phi(p^3) = p^3 - p^2$.

If $n = pq$ are distinct primes then $\phi(pq) =$

Totient Function

Will use the Euler totient function $\phi(n)$ later.
$\phi(n)$ is the number of numbers from 1 to n that are relatively prime to n.

If p prime, $\phi(p) = p - 1$.

If $n = p^2$, $\phi(p^2) = p^2 - p$ (lose $p, 2p, 3p, \ldots, p^2$.

If $n = p^3$, $\phi(p^3) = p^3 - p^2$.

If $n = pq$ are distinct primes then $\phi(pq) = (p-1)(q-1)$:

- Lose $p, 2p, 3p, \ldots, qp$.
- Lose $q, 2q, 3q, \ldots, pq$.
- Double counted pq so add back: $pq - q - p + 1 = (p-1)(q-1)$.

Vigenére, and Permutation Ciphers

Vigenére

Issue is always send a letter to same new letter....

Take a keyphrase, write under and use for shifts:

D A D C A N A D D A B E D

A B C A B C A B C A B C A

E C G D C Q B F G B D H E

So D shifted to E, F, G; A shifted to B, C; ....
How secure is this?

Vigenére

How secure is the Vigenére cipher?

- https://www.telegraph.co.uk/news/worldnews/northamerica/usa/8225871/CIA-decodes-Civil-War-message-in-a-bottle-after-147-years.html
- https://owlcation.com/humanities/1863-Siege-of-Vicksburg-Secret-Message-Decoded
- http://archive.boston.com/news/nation/articles/2010/12/26/civil_war_note_finally_deciphered/
- http://cryptiana.web.fc2.com/code/civilwar4.htm
- https://en.wikipedia.org/wiki/Kasiski_examination

Permutation Ciphers

26 choices for A, 25 for B, ...

$26! \approx$

Permutation Ciphers

26 choices for A, 25 for B, ...

$26! \approx 4 \cdot 10^{26}$.

A lot more than affine case!

How secure are these?

Frequency Attacks

1	e	12.58%	14	m	2.56%
2	t	9.09%	15	f	2.35%
3	a	8.00%	16	w	2.22%
4	o	7.59%	17	g	1.98%
5	i	6.92%	18	y	1.90%
6	n	6.90%	19	p	1.80%
7	s	6.34%	20	b	1.54%
8	h	6.24%	21	v	0.98%
9	r	5.96%	22	k	0.74%
10	d	4.32%	23	x	0.18%
11	l	4.06%	24	j	0.15%
12	u	2.84%	25	q	0.12%
13	c	2.58%	26	z	0.08%

TABLE 1. Frequencies of letters in English text, from 9,481 English works from Project Gutenberg; see http://www.cryptograms.org/letter-frequencies.php.

Frequency Attacks

most common bigrams	
1	th
2	he
3	in
4	en
5	nt
6	re
7	er
8	an
9	ti
10	es
11	on
12	at
13	se
14	nd
15	or
16	ar
17	al

common trigrams	
1	the
2	and
3	tha
4	ent
5	ing
6	ion
7	tio
8	for
9	nde
10	has
11	nce
12	edt
13	tis
14	oft
15	sth

Why Primes?

Two Systems

p, q are 200 digit primes, $N = pq$ public, password p **or** q.

X is a 5000 digit random number, password is X.

The more secure system is

Two Systems

p, q are 200 digit primes, $N = pq$ public, password p **or** q.

X is a 5000 digit random number, password is X.

The more secure system is the first (know it when here it, versus have to know).

Two Systems

p, q are 200 digit primes, $N = pq$ public, password p **or** q.

X is a 5000 digit random number, password is X.

The more secure system is the first (know it when here it, versus have to know).

Say every atom in the universe (about 10^{80} such) is a universe, and each atom there is a supercomputer checking 10^{15} items a second. About $3.2 \cdot 10^7$ seconds in a year, check about $3.2 \cdot 10^{182}$ per year.

Universe about 15 billion years old, so in the life of the universe would check about $5 \cdot 10^{192}$. Less than the number of primes to check!

RSA Description
(Rivest, Shamir, and Adleman)

Set-up: Example

Alice always sends to Bob, Charlie or Eve tries to intercept.

Bob does the following (could have b subscripts):

- Secret: $p = 15217$, $q = 17569$, $d = 80998505$.

Set-up: Example

Alice always sends to Bob, Charlie or Eve tries to intercept.

Bob does the following (could have b subscripts):

- Secret: $p = 15217$, $q = 17569$, $d = 80998505$.
- Public: $N = pq = 267347473$, $e = 3141593$.

Set-up: Example

Alice always sends to Bob, Charlie or Eve tries to intercept.

Bob does the following (could have *b* subscripts):

- Secret: $p = 15217$, $q = 17569$, $d = 80998505$.
- Public: $N = pq = 267347473$, $e = 3141593$.
- Note: $ed = 1 \bmod (p-1)(q-1)$.

Set-up: Example

Alice always sends to Bob, Charlie or Eve tries to intercept.

Bob does the following (could have b subscripts):

- Secret: $p = 15217$, $q = 17569$, $d = 80998505$.
- Public: $N = pq = 267347473$, $e = 3141593$.
- Note: $ed = 1 \bmod (p-1)(q-1)$.
- **Message:** $M = 195632041$**, send** $M^e \bmod N$ **or** $X = 121209473$**.**

Set-up: Example

Alice always sends to Bob, Charlie or Eve tries to intercept.

Bob does the following (could have b subscripts):

- Secret: $p = 15217$, $q = 17569$, $d = 80998505$.
- Public: $N = pq = 267347473$, $e = 3141593$.
- Note: $ed = 1 \bmod (p-1)(q-1)$.
- **Message:** $M = 195632041$**, send** $M^e \bmod N$ **or** $X = 121209473$**.**
- Decrypt: $X^d \bmod N$ or 195632041.

Set-up: Example

Alice always sends to Bob, Charlie or Eve tries to intercept.

Bob does the following (could have b subscripts):

- Secret: $p = 15217$, $q = 17569$, $d = 80998505$.
- Public: $N = pq = 267347473$, $e = 3141593$.
- Note: $ed = 1 \bmod (p-1)(q-1)$.
- **Message:** $M = 195632041$**, send** $M^e \bmod N$ **or** $X = 121209473$**.**
- Decrypt: $X^d \bmod N$ or 195632041.

Imagine receive $\widetilde{X} = 121209483$.
Message 195632041
Decrypts 121141028, only two digits are the same!

Implementation Questions

A lot of implementation issues.

- How do we find large primes? How large is large?
- How do we find e and d so that $ed = 1 \bmod (p-1)(q-1)$?
- How do we compute $M^e \bmod N$ efficiently?
- Can Eve determine d from e and N?