Modular Arithmetic and Cryptography

Recall

- Steganography - hide messages

Recall

- Steganography - hide messages
- Cryptography - scramble messages

Recall

- Steganography - hide messages
- Cryptography - scramble messages
- Transposition - rearrange symbols

Recall

- Steganography - hide messages
- Cryptography - scramble messages
- Transposition - rearrange symbols
- Column scytale, Columnar transposition

Recall

- Steganography - hide messages
- Cryptography - scramble messages
- Transposition - rearrange symbols
- Column scytale, Columnar transposition
- Substitution - replace symbols

Recall

- Steganography - hide messages
- Cryptography - scramble messages
- Transposition - rearrange symbols
- Column scytale, Columnar transposition
- Substitution - replace symbols
- Caesar Cipher, Atbash, Substitution with keyword

Recall

- Steganography - hide messages
- Cryptography - scramble messages
- Transposition - rearrange symbols
- Column scytale, Columnar transposition
- Substitution - replace symbols
- Caesar Cipher, Atbash, Substitution with keyword
- Frequency analysis

A time question

If it is 7:00 now, what time will it be in 8 hours?

A time question

If it is 7:00 now, what time will it be in 8 hours?

- $7 + 8 = 15$

A time question

If it is 7:00 now, what time will it be in 8 hours?

- $7 + 8 = 15$
- 15 is “too big” subtract 12

A time question

If it is 7:00 now, what time will it be in 8 hours?

- $7 + 8 = 15$
- 15 is "too big" subtract 12
- In 8 hours it will be 3:00.

A time question

If it is 7:00 now, what time will it be in 19 hours?

A time question

If it is 7:00 now, what time will it be in 19 hours?

- $7 + 19 = 26$

A time question

If it is 7:00 now, what time will it be in 19 hours?

- $7 + 19 = 26$
- 26 is too big

A time question

If it is 7:00 now, what time will it be in 19 hours?

- $7 + 19 = 26$
- 26 is too big
- $26 - 12 = 14$

A time question

If it is 7:00 now, what time will it be in 19 hours?

- $7 + 19 = 26$
- 26 is too big
- $26 - 12 = 14$ still too big
- $14 - 12 = 2$

A time question

If it is 7:00 now, what time will it be in 19 hours?

- $7 + 19 = 26$
- 26 is too big
- $26 - 12 = 14$ still too big
- $14 - 12 = 2$
- In 19 hours, it will be 2:00.

A time question

If it is 7:00 now, what time will it be in 100 hours?

A time question

If it is 7:00 now, what time will it be in 100 hours?

- $7 + 100 = 107$

A time question

If it is 7:00 now, what time will it be in 100 hours?

- $7 + 100 = 107$
- We could subtract repeatedly...

A time question

If it is 7:00 now, what time will it be in 100 hours?

- $7 + 100 = 107$
- We could subtract repeatedly...
- Repeated subtraction is (more or less) division.

A time question

If it is 7:00 now, what time will it be in 100 hours?

- $7 + 100 = 107$
- We could subtract repeatedly...
- Repeated subtraction is (more or less) division.
- What is left over after repeatedly subtracting 12 is the remainder when dividing by 12

A time question

If it is 7:00 now, what time will it be in 100 hours?

- $7 + 100 = 107$
- We could subtract repeatedly...
- Repeated subtraction is (more or less) division.
- What is left over after repeatedly subtracting 12 is the remainder when dividing by 12
- $107 \div 12$ is 9 with a remainder of 11

A time question

If it is 7:00 now, what time will it be in 100 hours?

- $7 + 100 = 107$
- We could subtract repeatedly...
- Repeated subtraction is (more or less) division.
- What is left over after repeatedly subtracting 12 is the remainder when dividing by 12
- $107 \div 12$ is 9 with a remainder of 11
- In 100 hours, it will be 11:00.

Mod

- There is nothing special about 12.
- If n is any positive integer and if m is any integer, then

$$m \pmod{n} \text{ is the remainder when } m \text{ is divided by } n.$$

- Note: The remainder should be one of $0, 1, 2, \ldots, (n-1)$.

Mods

$$17 \pmod{5} \quad =$$

Mods

$$17 \pmod 5 = 2$$

Mods

$$\begin{aligned}17 \pmod 5 &= 2\\ 96 \pmod{10} &=\end{aligned}$$

Mods

$$\begin{aligned} 17 \pmod{5} &= 2 \\ 96 \pmod{10} &= 6 \end{aligned}$$

Mods

$$\begin{aligned} 17 &\pmod{5} &= 2 \\ 96 &\pmod{10} &= 6 \\ 92 &\pmod{11} &= \end{aligned}$$

Mods

$$\begin{aligned} 17 \pmod{5} &= 2 \\ 96 \pmod{10} &= 6 \\ 92 \pmod{11} &= 3 \end{aligned}$$

Mods

$$
\begin{aligned}
17 \pmod 5 &= 2 \\
96 \pmod{10} &= 6 \\
92 \pmod{11} &= 3 \\
48 \pmod 4 &=
\end{aligned}
$$

Mods

$$\begin{aligned}
17 \pmod 5 &= 2 \\
96 \pmod{10} &= 6 \\
92 \pmod{11} &= 3 \\
48 \pmod 4 &= 0
\end{aligned}$$

Using a calculator

Find $12345 \pmod{678}$

Using a calculator

Find $12345 \pmod{678}$

- My calculator says $12345 \div 678 = 18.20796460176991150442477876106\,2$

Using a calculator

Find $12345 \pmod{678}$

- My calculator says
  $12345 \div 678 = 18.2079646017699115044247787610 62$
- Subtract 18 to get: 0.207964601769911504424778761061 95

Using a calculator

Find 12345 $\pmod{678}$

- My calculator says
  $12345 \div 678 = 18.2079646017699115044247787610 62$
- Subtract 18 to get: 0.20796460176991150442477876106195
- Multiply by 678 to get the remainder: 141

Using a calculator

Find $12345 \pmod{678}$

- My calculator says
  $12345 \div 678 = 18.207964601769911504424778761062$
- Subtract 18 to get: $0.20796460176991150442477876106195$
- Multiply by 678 to get the remainder: 141
- Note, you may have to round.

Using a calculator

$$1237 \pmod{12} =$$

Using a calculator

$$1237 \pmod{12} = 1$$

Using a calculator

$$
\begin{aligned}
1237 \pmod{12} &= 1 \\
87687 \pmod{77} &=
\end{aligned}
$$

Using a calculator

$$\begin{aligned} 1237 \pmod{12} &= 1 \\ 87687 \pmod{77} &= 61 \end{aligned}$$

Using a calculator

$$\begin{aligned} 1237 \quad &\pmod{12} &=& \quad 1 \\ 87687 \quad &\pmod{77} &=& \quad 61 \\ 987654 \quad &\pmod{9} &=& \end{aligned}$$

Using a calculator

$$\begin{aligned} 1237 \pmod{12} &= 1 \\ 87687 \pmod{77} &= 61 \\ 987654 \pmod{9} &= 3 \end{aligned}$$

Calendars

The ancient Chinese invented modular arithmetic to answer questions like:
Today is Thursday, April 12, 2018. What day of the week will April 12, 2018 be?

Calendars

The ancient Chinese invented modular arithmetic to answer questions like:
Today is Thursday, April 12, 2018. What day of the week will April 12, 2018 be?

- Treat days like numbers 0=Sunday, 1=Monday, 2=Tuesday...

Calendars

The ancient Chinese invented modular arithmetic to answer questions like:
Today is Thursday, April 12, 2018. What day of the week will April 12, 2018 be?

- Treat days like numbers 0=Sunday, 1=Monday, 2=Tuesday...
- Today is a 4

Calendars

The ancient Chinese invented modular arithmetic to answer questions like:
Today is Thursday, April 12, 2018. What day of the week will April 12, 2018 be?

- Treat days like numbers 0=Sunday, 1=Monday, 2=Tuesday...
- Today is a 4
- We are looking for $4 + 365 \pmod 7 = 5$

Calendars

The ancient Chinese invented modular arithmetic to answer questions like:
Today is Thursday, April 12, 2018. What day of the week will April 12, 2018 be?

- Treat days like numbers 0=Sunday, 1=Monday, 2=Tuesday...
- Today is a 4
- We are looking for $4 + 365 \pmod 7 = 5$
- Friday.

- If n is a positive integer, $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$

$\mathbb{Z}_n$

- If n is a positive integer, $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$
- (The remainders mod n.)

$\mathbb{Z}_n$

- If n is a positive integer, $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$
- (The remainders mod n.)
- $\mathbb{Z}_2 = \{0, 1\}$

- If n is a positive integer, $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$
- (The remainders mod n.)
- $\mathbb{Z}_2 = \{0, 1\}$
- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$\mathbb{Z}_n$

- If n is a positive integer, $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$
- (The remainders mod n.)
- $\mathbb{Z}_2 = \{0, 1\}$
- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
- In $\mathbb{Z}_n$, we can do arithmetic mod n.

$\mathbb{Z}_n$

- If n is a positive integer, $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$
- (The remainders mod n.)
- $\mathbb{Z}_2 = \{0, 1\}$
- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
- In $\mathbb{Z}_n$, we can do arithmetic mod n.
- This gives a small number system - with only n numbers.

$\mathbb{Z}_n$

- If n is a positive integer, $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$
- (The remainders mod n.)
- $\mathbb{Z}_2 = \{0, 1\}$
- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
- In $\mathbb{Z}_n$, we can do arithmetic mod n.
- This gives a small number system - with only n numbers.
- We can do much of our usual arithmetic and algebra in $\mathbb{Z}_n$

Addition and Multiplication in $\mathbb{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

An equation in $\mathbb{Z}_5$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_5$.

An equation in $\mathbb{Z}_5$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_5$.
- Subtract 1 to get $2x = 3$

An equation in $\mathbb{Z}_5$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_5$.
- Subtract 1 to get $2x = 3$
- Note that $3 \times 2 = 1$, so

An equation in $\mathbb{Z}_5$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_5$.
- Subtract 1 to get $2x = 3$
- Note that $3 \times 2 = 1$, so
- Multiply by 3 to get $3 \times 2x = 3 \times 3$

An equation in $\mathbb{Z}_5$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_5$.
- Subtract 1 to get $2x = 3$
- Note that $3 \times 2 = 1$, so
- Multiply by 3 to get $3 \times 2x = 3 \times 3$
- This is the same as $1x = 4$ or $x = 4$

An equation in $\mathbb{Z}_6$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_6$

An equation in $\mathbb{Z}_6$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_6$
- Subtract 1 to get $2x = 3$

An equation in $\mathbb{Z}_6$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_6$
- Subtract 1 to get $2x = 3$
- Look for a multiplicative inverse of 2 in $\mathbb{Z}_6$....

An equation in $\mathbb{Z}_6$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_6$
- Subtract 1 to get $2x = 3$
- Look for a multiplicative inverse of 2 in $\mathbb{Z}_6$....
- Try brute force: $2 \times 0 = 0$, $2 \times 1 = 2$, $2 \times 2 = 4$, $2 \times 3 = 0$, $2 \times 4 = 2$, $2 \times 5 = 4$

An equation in $\mathbb{Z}_6$

- Solve $2x + 1 = 4$ in $\mathbb{Z}_6$
- Subtract 1 to get $2x = 3$
- Look for a multiplicative inverse of 2 in $\mathbb{Z}_6$....
- Try brute force: $2 \times 0 = 0$, $2 \times 1 = 2$, $2 \times 2 = 4$, $2 \times 3 = 0$, $2 \times 4 = 2$, $2 \times 5 = 4$
- There is no solution to this equation in $\mathbb{Z}_6$.

Weird

In $\mathbb{Z}_6$, $2 \times 3 = 0$

Weird

In $\mathbb{Z}_6$, $2 \times 3 = 0$

2 and 3 are divisors of 0

An equation in $\mathbb{Z}_5$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_5$

An equation in $\mathbb{Z}_5$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_5$
- Factor to get $(x + 2)(x + 1) = 0$

An equation in $\mathbb{Z}_5$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_5$
- Factor to get $(x + 2)(x + 1) = 0$
- In $\mathbb{Z}_5$, the only products that are 0 involve a factor of 0

An equation in $\mathbb{Z}_5$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_5$
- Factor to get $(x + 2)(x + 1) = 0$
- In $\mathbb{Z}_5$, the only products that are 0 involve a factor of 0
- This means $x + 2 = 0$ or $x + 1 = 0$

An equation in $\mathbb{Z}_5$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_5$
- Factor to get $(x+2)(x+1) = 0$
- In $\mathbb{Z}_5$, the only products that are 0 involve a factor of 0
- This means $x + 2 = 0$ or $x + 1 = 0$
- $x = 3$ or $x = 4$

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$
- Factor to get $(x + 2)(x + 1) = 0$

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$
- Factor to get $(x + 2)(x + 1) = 0$
- But in $\mathbb{Z}_6$, the products of some non-zero numbers is 0!

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$
- Factor to get $(x+2)(x+1) = 0$
- But in $\mathbb{Z}_6$, the products of some non-zero numbers is 0!
- This does not help!

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$ by BRUTE FORCE

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$ by BRUTE FORCE
- $0^2 + 3 \times 0 + 2 = 2$ so 0 is not a solution

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$ by BRUTE FORCE
- $0^2 + 3 \times 0 + 2 = 2$ so 0 is not a solution
- $1^2 + 3 \times 1 + 2 = 0$ so 1 is a solution

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$ by BRUTE FORCE
- $0^2 + 3 \times 0 + 2 = 2$ so 0 is not a solution
- $1^2 + 3 \times 1 + 2 = 0$ so 1 is a solution
- $2^2 + 3 \times 2 + 2 = 0$ so 2 is a solution

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$ by BRUTE FORCE
- $0^2 + 3 \times 0 + 2 = 2$ so 0 is not a solution
- $1^2 + 3 \times 1 + 2 = 0$ so 1 is a solution
- $2^2 + 3 \times 2 + 2 = 0$ so 2 is a solution
- $3^2 + 3 \times 3 + 2 = 2$ so 3 is not a solution

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$ by BRUTE FORCE
- $0^2 + 3 \times 0 + 2 = 2$ so 0 is not a solution
- $1^2 + 3 \times 1 + 2 = 0$ so 1 is a solution
- $2^2 + 3 \times 2 + 2 = 0$ so 2 is a solution
- $3^2 + 3 \times 3 + 2 = 2$ so 3 is not a solution
- $4^2 + 3 \times 4 + 2 = 0$ so 4 is a solution

An equation in $\mathbb{Z}_6$

- Solve $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$ by BRUTE FORCE
- $0^2 + 3 \times 0 + 2 = 2$ so 0 is not a solution
- $1^2 + 3 \times 1 + 2 = 0$ so 1 is a solution
- $2^2 + 3 \times 2 + 2 = 0$ so 2 is a solution
- $3^2 + 3 \times 3 + 2 = 2$ so 3 is not a solution
- $4^2 + 3 \times 4 + 2 = 0$ so 4 is a solution
- $5^2 + 3 \times 5 + 2 = 0$ so 5 is a solution

Another oddity

In $\mathbb{Z}_{17}$, there is a solution to $x^2 + 1 = 0$.

Another oddity

In $\mathbb{Z}_{17}$, there is a solution to $x^2 + 1 = 0$.

This does not happen in the real numbers.

Back to cryptography

Letters and numbers

We can identify letters and numbers:

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

Letters and numbers

Identify the alphabet with $\mathbb{Z}_{26}$ and can do arithmetic with letters.

Letter calculations

Calculate:

- P+W=

Letter calculations

Calculate:

- $P+W=L$
- $H \times C=$

Letter calculations

Calculate:

- $P+W=L$
- $H\times C=O$
- $F\times(E+K)=$

Letter calculations

Calculate:

- $P+W=L$
- $H\times C=O$
- $F\times(E+K)=F\times O=$

Letter calculations

Calculate:

- P+W=L
- H×C=O
- F×(E+K)=F×O=S

Caesar Cipher

A Caesar cipher with key k replaces any plaintext letter p with $p + k$.

- Encrypt "cat" with a Caesar Cipher and key D

A Caesar cipher with key k replaces any plaintext letter p with $p + k$.

- Encrypt “cat” with a Caesar Cipher and key D
- Add

$$\begin{array}{rccc} & \text{c} & \text{a} & \text{t} \\ + & \text{D} & \text{D} & \text{D} \\ \hline & \text{F} & \text{D} & \text{W} \end{array}$$

Caesar Cipher

A Caesar cipher with key k replaces any plaintext letter p with $p + k$.

- Encrypt "cat" with a Caesar Cipher and key D
- Add

$$\begin{array}{cccc} & \text{c} & \text{a} & \text{t} \\ + & \text{D} & \text{D} & \text{D} \\ \hline & \text{F} & \text{D} & \text{W} \end{array}$$

- Ciphertext: FDW

Caesar Cipher

A Caesar cipher with key k replaces any plaintext letter p with $p + k$.

- Encrypt "cat" with a Caesar Cipher and key D
- Add

$$\begin{array}{cccc} & \mathsf{c} & \mathsf{a} & \mathsf{t} \\ + & \mathsf{D} & \mathsf{D} & \mathsf{D} \\ \hline & \mathsf{F} & \mathsf{D} & \mathsf{W} \end{array}$$

- Ciphertext: FDW
- To decypt, subtract.

$$\begin{array}{cccc} & \mathsf{F} & \mathsf{D} & \mathsf{W} \\ - & \mathsf{D} & \mathsf{D} & \mathsf{D} \\ \hline & \mathsf{c} & \mathsf{a} & \mathsf{t} \end{array}$$

Atbash

Atbash encrypts any plaintext letter p as $Z - p$.

- Encrypt "holy"

Atbash

Atbash encrypts any plaintext letter p as $Z - p$.

- Encrypt "holy"
- Subtract

	Z	Z	Z	Z
-	h	o	l	y
	S	L	O	B

Atbash

Atbash encrypts any plaintext letter p as $Z - p$.

- Encrypt "holy"
- Subtract

$$\begin{array}{ccccc} & Z & Z & Z & Z \\ - & h & o & l & y \\ \hline & S & L & O & B \end{array}$$

- Ciphertext: SLOB

Atbash

Atbash encrypts any plaintext letter p as $Z - p$.

- Encrypt "holy"
- Subtract

$$\begin{array}{ccccc} & Z & Z & Z & Z \\ - & h & o & l & y \\ \hline & S & L & O & B \end{array}$$

- Ciphertext: SLOB
- Decrypt also by subtracting from ZZZZZZ

Virtually every modern cipher system uses modular arithmetic...

Virtually every modern cipher system uses modular arithmetic...because computers are designed to do modular arithmetic...

Virtually every modern cipher system uses modular arithmetic...because computers are designed to do modular arithmetic...more on that later...

Improvements to Simple Substitution

- Null characters - random, meaningless symbols inserted in ciphertext to skew frequency analysis.

Improvements to Simple Substitution

- Null characters - random, meaningless symbols inserted in ciphertext to skew frequency analysis.
- Mispld werds tu chanj fwikwincees

Improvements to Simple Substitution

- Null characters - random, meaningless symbols inserted in ciphertext to skew frequency analysis.
- Mispld werds tu chanj fwikwincees
- Use some symbols to represent entire words.

Improvements to Simple Substitution

- Null characters - random, meaningless symbols inserted in ciphertext to skew frequency analysis.
- Mispld werds tu chanj fwikwincees
- Use some symbols to represent entire words.
- Substitution for syllables rather than letters

Improvements to Simple Substitution

- Null characters - random, meaningless symbols inserted in ciphertext to skew frequency analysis.
- Mispld werds tu chanj fwikwincees
- Use some symbols to represent entire words.
- Substitution for syllables rather than letters
- Substitution for pairs of letters rather than single letters

Improvements to Simple Substitution

- Null characters - random, meaningless symbols inserted in ciphertext to skew frequency analysis.
- Mispld werds tu chanj fwikwincees
- Use some symbols to represent entire words.
- Substitution for syllables rather than letters
- Substitution for pairs of letters rather than single letters
- Homophonic substitution - more than one symbol can be used to represent a plaintext letter

Homophonic substitution cipher

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
09	48	13	10	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

t	u	r	n		t	o		t	h	e		e	a	s	t
17	08	29	18		20	00		30	23	14		16	09	11	43

Mono- vs. Poly-Alphabetic

- Mono-alphabetic substitution:

- Mono-alphabetic substitution:
  - Every occurrence of a letter in the plaintext is encrypted with the same ciphertext symbol (or)

Mono- vs. Poly-Alphabetic

- Mono-alphabetic substitution:
  - Every occurrence of a letter in the plaintext is encrypted with the same ciphertext symbol (or)
  - Every occurrence of a symbol in the ciphertext represents the same plaintext letter.

Mono- vs. Poly-Alphabetic

- Mono-alphabetic substitution:
  - Every occurrence of a letter in the plaintext is encrypted with the same ciphertext symbol (or)
  - Every occurrence of a symbol in the ciphertext represents the same plaintext letter.
- Poly-alphabetic substitution:

Mono- vs. Poly-Alphabetic

- Mono-alphabetic substitution:
  - Every occurrence of a letter in the plaintext is encrypted with the same ciphertext symbol (or)
  - Every occurrence of a symbol in the ciphertext represents the same plaintext letter.
- Poly-alphabetic substitution:
  - A plaintext letter may be encrypted multiple ways.

Mono- vs. Poly-Alphabetic

- Mono-alphabetic substitution:
  - Every occurrence of a letter in the plaintext is encrypted with the same ciphertext symbol (or)
  - Every occurrence of a symbol in the ciphertext represents the same plaintext letter.
- Poly-alphabetic substitution:
  - A plaintext letter may be encrypted multiple ways.
  - A ciphertext symbol may represent different plaintext letters.

Viginère

- In 1586 Blaise de Viginère published a treatise describing a poly-alphabetic cipher which was a vast improvement over every mono-alphabetic cipher in use.

Viginère

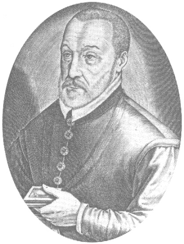
- In 1586 Blaise de Viginère published a treatise describing a poly-alphabetic cipher which was a vast improvement over every mono-alphabetic cipher in use.
- The Viginère cipher is a simple improvement on the Caesar Cipher.

Viginère

- In 1586 Blaise de Viginère published a treatise describing a poly-alphabetic cipher which was a vast improvement over every mono-alphabetic cipher in use.
- The Viginère cipher is a simple improvement on the Caesar Cipher.
- The Viginère cipher was not widely accepted because it was somewhat tedious (even though machines like Alberti's wheel made it easier).

Viginère

- In 1586 Blaise de Viginère published a treatise describing a poly-alphabetic cipher which was a vast improvement over every mono-alphabetic cipher in use.
- The Viginère cipher is a simple improvement on the Caesar Cipher.
- The Viginère cipher was not widely accepted because it was somewhat tedious (even though machines like Alberti's wheel made it easier).
- A mod-2 version of the Viginère cipher is present in many modern ciphers.



Caesar Cipher

Recall...

- To encrypt "secret message" with a key of D
- Add D to each letter of the plaintext:

	s	e	c	r	e	t	m	e	s	s	a	g	e
+	D	D	D	D	D	D	D	D	D	D	D	D	D
	V	H	F	U	H	W	P	H	V	V	D	J	H

- Every e is encrypted as H.
- Every H represents an e.
- Decrypt by subtracting D.

Viginère suggested that instead of adding a SINGLE LETTER to the plaintext, we could add a WORD.

Viginère

- To encrypt "secret message" with a key of MATH

Viginère

- To encrypt "secret message" with a key of MATH
- Copy MATH repeatedly under the plaintext and add

	s	e	c	r	e	t	m	e	s	s	a	g	e
+	M	A	T	H	M	A	T	H	M	A	T	H	M
	E	E	V	Y	Q	T	F	L	E	S	T	N	Q

Viginère

- To encrypt "secret message" with a key of MATH
- Copy MATH repeatedly under the plaintext and add

	s	e	c	r	e	t	m	e	s	s	a	g	e
+	M	A	T	H	M	A	T	H	M	A	T	H	M
	E	E	V	Y	Q	T	F	L	E	S	T	N	Q

- The e's are encrypted as E, Q, L

Viginère

- To encrypt "secret message" with a key of MATH
- Copy MATH repeatedly under the plaintext and add

	s	e	c	r	e	t	m	e	s	s	a	g	e
+	M	A	T	H	M	A	T	H	M	A	T	H	M
	E	E	V	Y	Q	T	F	L	E	S	T	N	Q

- The e's are encrypted as E, Q, L
- E represents both s and e

Viginère

- To encrypt "secret message" with a key of MATH
- Copy MATH repeatedly under the plaintext and add

	s	e	c	r	e	t	m	e	s	s	a	g	e
+	M	A	T	H	M	A	T	H	M	A	T	H	M
	E	E	V	Y	Q	T	F	L	E	S	T	N	Q

- The e's are encrypted as E, Q, L
- E represents both s and e
- Decrypt by subtracting the keyword.

Viginère

- To encrypt "secret message" with a key of MATH
- Copy MATH repeatedly under the plaintext and add

	s	e	c	r	e	t	m	e	s	s	a	g	e
+	M	A	T	H	M	A	T	H	M	A	T	H	M
	E	E	V	Y	Q	T	F	L	E	S	T	N	Q

- The e's are encrypted as E, Q, L
- E represents both s and e
- Decrypt by subtracting the keyword.
- Frequency analysis is hard (but not impossible)

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.
- Try random keys to decrypt the message.

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.
- Try random keys to decrypt the message.
    - Try ABCDEFG

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.
- Try random keys to decrypt the message.
  - Try ABCDEFG
  - Try ABXDBFG

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.
- Try random keys to decrypt the message.
  - Try ABCDEFG
  - Try ABXDBFG
  - Try FPCEVLN

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.
- Try random keys to decrypt the message.
    - Try ABCDEFG
    - Try ABXDBFG
    - Try FPCEVLN
    - Try RVMONLH

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.
- Try random keys to decrypt the message.
  - Try ABCDEFG
  - Try ABXDBFG
  - Try FPCEVLN
  - Try RVMONLH
  - Try EBCPHHK

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.
- Try random keys to decrypt the message.
    - Try ABCDEFG
    - Try ABXDBFG
    - Try FPCEVLN
    - Try RVMONLH
    - Try EBCPHHK
- Every seven letter message is possible.

Viginère with long keys

- Interesting things happen with Viginère if the key is random and is as long as the plaintext.
- The ciphertext GPPRVYN was encrypted with a Viginère cipher with a key longer than the plaintext.
- Try random keys to decrypt the message.
  - Try ABCDEFG
  - Try ABXDBFG
  - Try FPCEVLN
  - Try RVMONLH
  - Try EBCPHHK
- Every seven letter message is possible.
- Decryption is PROVABLY IMPOSSIBLE!

One Time Pad

- The only PROVABLE SECURE cipher in existence.

One Time Pad

- The only PROVABLE SECURE cipher in existence.
- Key = a "pad" of pages of random letters.

One Time Pad

- The only PROVABLE SECURE cipher in existence.
- Key = a "pad" of pages of random letters.
- Sender/Receiver begin on the same page of the pad and discard that page after it is used.

One Time Pad

- The only PROVABLE SECURE cipher in existence.
- Key $=$ a "pad" of pages of random letters.
- Sender/Receiver begin on the same page of the pad and discard that page after it is used.
- Used between Moscow and Washington for decades.

One Time Pad

- The only PROVABLE SECURE cipher in existence.
- Key = a "pad" of pages of random letters.
- Sender/Receiver begin on the same page of the pad and discard that page after it is used.
- Used between Moscow and Washington for decades.
- As long as

One Time Pad

- The only PROVABLE SECURE cipher in existence.
- Key = a "pad" of pages of random letters.
- Sender/Receiver begin on the same page of the pad and discard that page after it is used.
- Used between Moscow and Washington for decades.
- As long as
  - The key is absolutely random

One Time Pad

- The only PROVABLE SECURE cipher in existence.
- Key = a "pad" of pages of random letters.
- Sender/Receiver begin on the same page of the pad and discard that page after it is used.
- Used between Moscow and Washington for decades.
- As long as
  - The key is absolutely random
  - The key is never re-used

One Time Pad

- The only PROVABLE SECURE cipher in existence.
- Key = a “pad” of pages of random letters.
- Sender/Receiver begin on the same page of the pad and discard that page after it is used.
- Used between Moscow and Washington for decades.
- As long as
  - The key is absolutely random
  - The key is never re-used
  - The key is as long as the plaintext

One Time Pad

- The only PROVABLE SECURE cipher in existence.
- Key = a "pad" of pages of random letters.
- Sender/Receiver begin on the same page of the pad and discard that page after it is used.
- Used between Moscow and Washington for decades.
- As long as
  - The key is absolutely random
  - The key is never re-used
  - The key is as long as the plaintext
- This is absolutely secure.

One Time Pad

- It is hard to generate sequences of random letters with no patterns. ANY PATTERN can be exploited.

One Time Pad

- It is hard to generate sequences of random letters with no patterns. ANY PATTERN can be exploited.
- Once the pad is generated, it has to be shared between the sender and receiver (Key Sharing Problem).

One Time Pad

- It is hard to generate sequences of random letters with no patterns. ANY PATTERN can be exploited.
- Once the pad is generated, it has to be shared between the sender and receiver (Key Sharing Problem).
    - Every cipher we have talked about has this problem.

One Time Pad

- It is hard to generate sequences of random letters with no patterns. ANY PATTERN can be exploited.
- Once the pad is generated, it has to be shared between the sender and receiver (Key Sharing Problem).
  - Every cipher we have talked about has this problem.
- Some have used the One Time Pad with their favorite novel as a key pad.

Breaking Viginère

- If the key for Viginère is shorter than the plaintext and repeated, then Viginère can be broken.
- If the key has length, say, 5, then every fifth letter is encrypted with a Caesar Cipher.
- A frequence analysis on every fifth letter would easily give the key.
- All that is needed is the key-length.
- The key-length can be found with some “statistical-voodoo”
- Methods developed independently by Charles Babbage and Wilhelm Kasiski around 1850

Crypto at the end of the nineteenth century

- Best cryptography methods in homophonic substitution and Viginère cipher.

Crypto at the end of the nineteenth century

- Best cryptography methods in homophonic substitution and Viginère cipher.
- Homophonic substitutions can be broken with complex frequency analysis.

Crypto at the end of the nineteenth century

- Best cryptography methods in homophonic substitution and Viginère cipher.
- Homophonic substitutions can be broken with complex frequency analysis.
- Babbage and Kasiski had discovered how to break Viginère around 1850.

Crypto at the end of the nineteenth century

- Best cryptography methods in homophonic substitution and Viginère cipher.
- Homophonic substitutions can be broken with complex frequency analysis.
- Babbage and Kasiski had discovered how to break Viginère around 1850.
- Radio brought the need for fast, mechanical encryption.

Column Scytale – Transposition Cipher

- To encrypt the plaintext "attack the south gate at dawn" with 5 columns

Column Scytale – Transposition Cipher

- To encrypt the plaintext "attack the south gate at dawn" with 5 columns
- Write the text in a grid of 5 columns:

a	t	t	a	c
k	t	h	e	s
o	u	t	h	g
a	t	e	a	t
d	a	w	n	x

  filling in extra space with gibberish.

Column Scytale – Transposition Cipher

- To encrypt the plaintext "attack the south gate at dawn" with 5 columns
- Write the text in a grid of 5 columns:

a	t	t	a	c
k	t	h	e	s
o	u	t	h	g
a	t	e	a	t
d	a	w	n	x

  filling in extra space with gibberish.
- Copy the ciphertext down the columns:

  AKOADTTUTATHTEWAEHANCSGTX

Tabular Substitution

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

- A letter is encrypted as a pair of symbols - the row and column containing the letter.

Tabular Substitution

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

- A letter is encrypted as a pair of symbols - the row and column containing the letter.
- Example: G is encrypted as FD

Combining

The most successful means of cryptography combine methods.

Tabular		Column		Collapse
Substitution	$\rightarrow$	Scytale	$\rightarrow$	Tabular
				Substitution

Example

- For the plaintext “attack at dawn”

Example

- For the plaintext “attack at dawn”
- Encrypt with a tabular substitution and the keyword ZEBRA

Example

- For the plaintext "attack at dawn"
- Encrypt with a tabular substitution and the keyword ZEBRA
- Encrypt the result of the previous step with a column scytale with 5 columns

Example

- For the plaintext "attack at dawn"
- Encrypt with a tabular substitution and the keyword ZEBRA
- Encrypt the result of the previous step with a column scytale with 5 columns
- Collapse the result of the last step with a tabular substitution with keyword ZIPF

ADFGX...ADFGVX

- Two of the most important German ciphers of WWI

ADFGX...ADFGVX

- Two of the most important German ciphers of WWI
- Consisted of a tabular substitution (with labels ADFG(V)X)

ADFGX...ADFGVX

- Two of the most important German ciphers of WWI
- Consisted of a tabular substitution (with labels ADFG(V)X)
- followed by a columnar transposition

ADFGX...ADFGVX

- Two of the most important German ciphers of WWI
- Consisted of a tabular substitution (with labels ADFG(V)X)
- followed by a columnar transposition
- (no collapse).

ADFGX...ADFGVX

- Two of the most important German ciphers of WWI
- Consisted of a tabular substitution (with labels ADFG(V)X)
- followed by a columnar transposition
- (no collapse).
- Breaking the ADFGVX cipher helped to prevent Germany from taking Paris.

Modern Times

Most modern ciphers include these ingredients:

- Break apart the letters of the plaintext into parts. (To diffuse information)

Modern Times

Most modern ciphers include these ingredients:

- Break apart the letters of the plaintext into parts. (To diffuse information)
- Rearrange and substitute the parts.

Modern Times

Most modern ciphers include these ingredients:

- Break apart the letters of the plaintext into parts. (To diffuse information)
- Rearrange and substitute the parts.
- Glue the parts back together.

- Guglielmo Marconi invented the radio at the turn of the century.

Radio and Cipher Machines

- Guglielmo Marconi invented the radio at the turn of the century.
- Contributed to the need for better/faster cryptographic methods.

Radio and Cipher Machines

- Guglielmo Marconi invented the radio at the turn of the century.
- Contributed to the need for better/faster cryptographic methods.
- Commanders could communicate directly and immediately with soldiers on the battleground.

Radio and Cipher Machines

- Guglielmo Marconi invented the radio at the turn of the century.
- Contributed to the need for better/faster cryptographic methods.
- Commanders could communicate directly and immediately with soldiers on the battleground.
- Anyone with a radio could intercept communications.

Radio and Cipher Machines

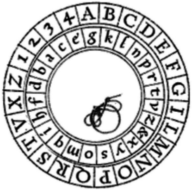
- Guglielmo Marconi invented the radio at the turn of the century.
- Contributed to the need for better/faster cryptographic methods.
- Commanders could communicate directly and immediately with soldiers on the battleground.
- Anyone with a radio could intercept communications.
- Ease of Communication vs. Ease of Interception.

Radio and Cipher Machines

- Guglielmo Marconi invented the radio at the turn of the century.
- Contributed to the need for better/faster cryptographic methods.
- Commanders could communicate directly and immediately with soldiers on the battleground.
- Anyone with a radio could intercept communications.
- Ease of Communication vs. Ease of Interception.
- Partially drove the movement toward mechanized cryptography.

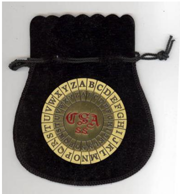
Alberti and the Cipher Disk

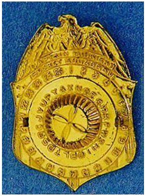
Almost five hundred years before WWI, Alberti made a "cipher disk" to help perform substitution ciphers (Caesar) more quickly.



Alberti and the Cipher Disk

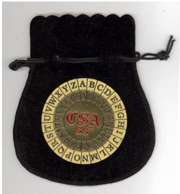
- The plain alphabet and cipher alphabet were written on two disks, one smaller than the other.

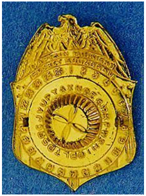




Alberti and the Cipher Disk

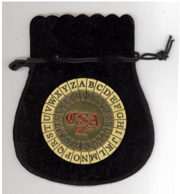
- The plain alphabet and cipher alphabet were written on two disks, one smaller than the other.
- The smaller disk was attached to the center of the larger disk.

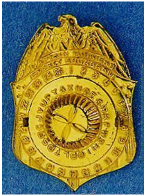




Alberti and the Cipher Disk

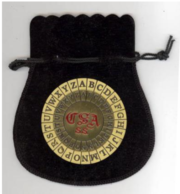
- The plain alphabet and cipher alphabet were written on two disks, one smaller than the other.
- The smaller disk was attached to the center of the larger disk.
- The smaller disk could be rotated to line up the plaintext "a" with a ciphertext letter (the key).

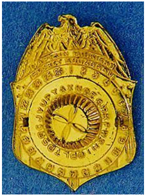




Alberti and the Cipher Disk

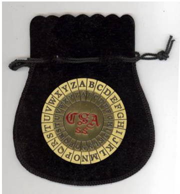
- The plain alphabet and cipher alphabet were written on two disks, one smaller than the other.
- The smaller disk was attached to the center of the larger disk.
- The smaller disk could be rotated to line up the plaintext "a" with a ciphertext letter (the key).
- Ciphertext letters lining up with plaintext could be read off the disk.

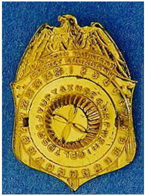




Alberti and the Cipher Disk

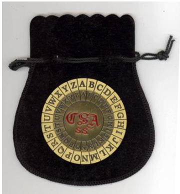
- The plain alphabet and cipher alphabet were written on two disks, one smaller than the other.
- The smaller disk was attached to the center of the larger disk.
- The smaller disk could be rotated to line up the plaintext “a” with a ciphertext letter (the key).
- Ciphertext letters lining up with plaintext could be read off the disk.
- You could rotate the inner disk after each letter to accomplish a poly-alphabetic substition (like Viginère).

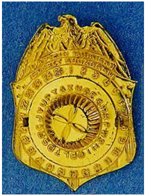




Alberti and the Cipher Disk

- The plain alphabet and cipher alphabet were written on two disks, one smaller than the other.
- The smaller disk was attached to the center of the larger disk.
- The smaller disk could be rotated to line up the plaintext “a” with a ciphertext letter (the key).
- Ciphertext letters lining up with plaintext could be read off the disk.
- You could rotate the inner disk after each letter to accomplish a poly-alphabetic substition (like Viginère).
- Predecessor of the most formidable cipher machine of WWII.





Arthur Scherbius and *the* Enigma

- In 1918 Arthur Scherbius started a company to build an electronic cryptography machine call Enigma.

Arthur Scherbius and *the* Enigma

- In 1918 Arthur Scherbius started a company to build an electronic cryptography machine call Enigma.
- He planned on selling the machine to businesses and governments.

Arthur Scherbius and *the* Enigma

- In 1918 Arthur Scherbius started a company to build an electronic cryptography machine call Enigma.
- He planned on selling the machine to businesses and governments.
- The machine was efficient, fast, and secure (by standards of the early 20th century).

Arthur Scherbius and *the* Enigma

- In 1918 Arthur Scherbius started a company to build an electronic cryptography machine call Enigma.
- He planned on selling the machine to businesses and governments.
- The machine was efficient, fast, and secure (by standards of the early 20th century).
- It was also over-priced.

Arthur Scherbius and *the* Enigma

- In 1918 Arthur Scherbius started a company to build an electronic cryptography machine call Enigma.
- He planned on selling the machine to businesses and governments.
- The machine was efficient, fast, and secure (by standards of the early 20th century).
- It was also over-priced.
- The only interested customer was the German government.

Arthur Scherbius and *the* Enigma

- In 1918 Arthur Scherbius started a company to build an electronic cryptography machine call Enigma.
- He planned on selling the machine to businesses and governments.
- The machine was efficient, fast, and secure (by standards of the early 20th century).
- It was also over-priced.
- The only interested customer was the German government.
- Others devised similar machines, but their businesses all failed.

Enigma