Mathematics and mathematical cryptography

Math workshop
May 12, 2017

Monica Nevins and Team
Department of Mathematics and Statistics

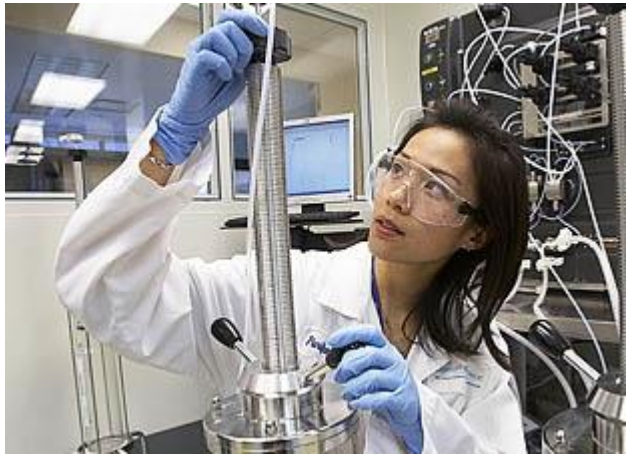
Mathematics

Question #1: Is Mathematics really Science?

Answer: Mathematics turned

Natural philosophers

into



scientists.

Mathematics is the **queen** of the sciences.*

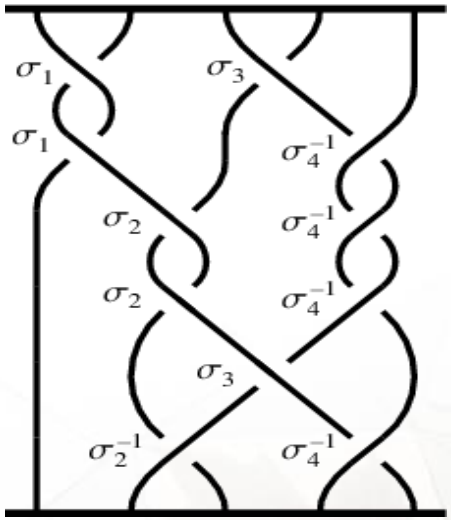
uOttawa

*Carl Friedrich Gauss, 1777-1855

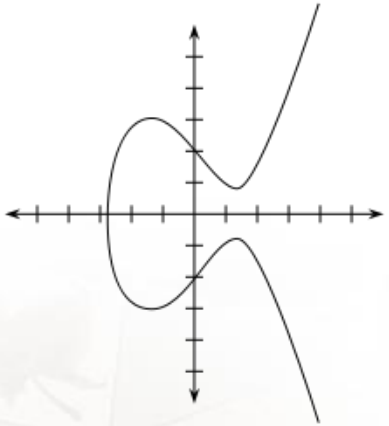
Mathematics

Question #2: Is there anything left to discover in mathematics?

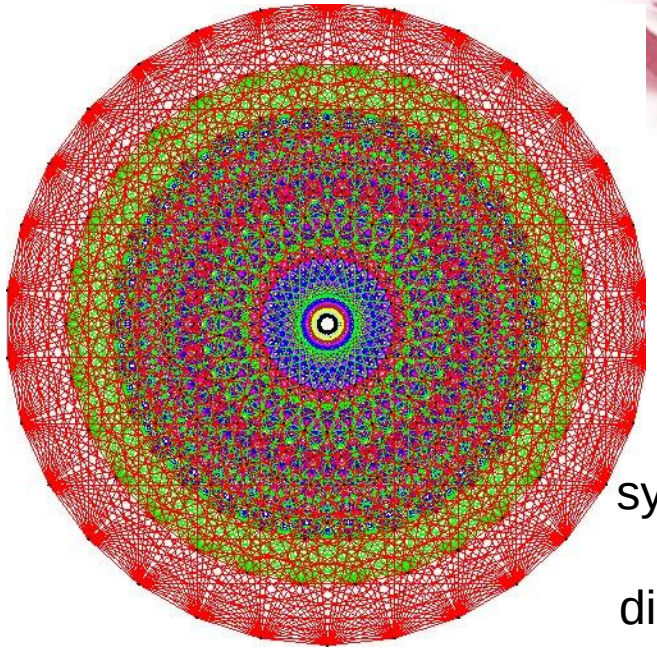
Answer: **Oh, yes!**



Braid groups

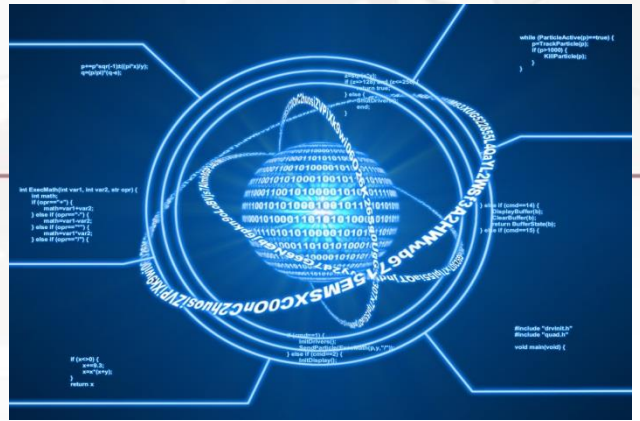


Elliptic curves



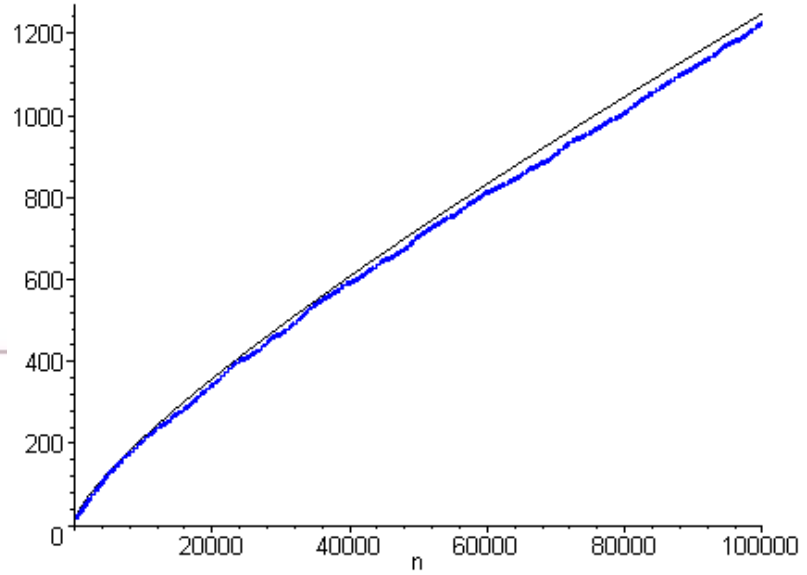
E_8

Lattice symmetries in high dimensions



Quantum computing

Twin primes conjecture



Question #3: What is mathematics?

Mathematics

is about

solving puzzles

and

finding patterns.

1, 2, 4, 8, 16, 32, 64, 128, 256, … Powers of 2

2, 3, 5, 7, 11, 13, 17, 19, 23, … Prime numbers

An example (due to Gauss, age 6)

https://en.wikipedia.org/wiki/Christian_Albrecht_Jensen

The teacher told the class to add up all the numbers from 1 to 100.

$1+2=3$

$1+2+3=6$

$1+2+3+4=10$

$1+2+3+4+5=15$

$1+2+3+4+5+6=21$

…

But Gauss looks for a pattern:

$$1+2+3+4+5+6$$

$$=7+7+7$$

$$=3\times 7$$

$$=21$$

Your turn: What is $1+2+3+\ldots+8+9+10$?

What is $1+2+3+\ldots+98+99+100$?

uOttawa

So that's math; what's cryptography?

Cryptography is the art and science of **obfuscating messages** so that none but the intended recipient can read them.

Good cryptography is any method that is reliable, easy for Alice and Bob to use, and produces **ciphertexts** that are impossible for Eve to figure out.

uOttawa

An example: the Caesar cipher

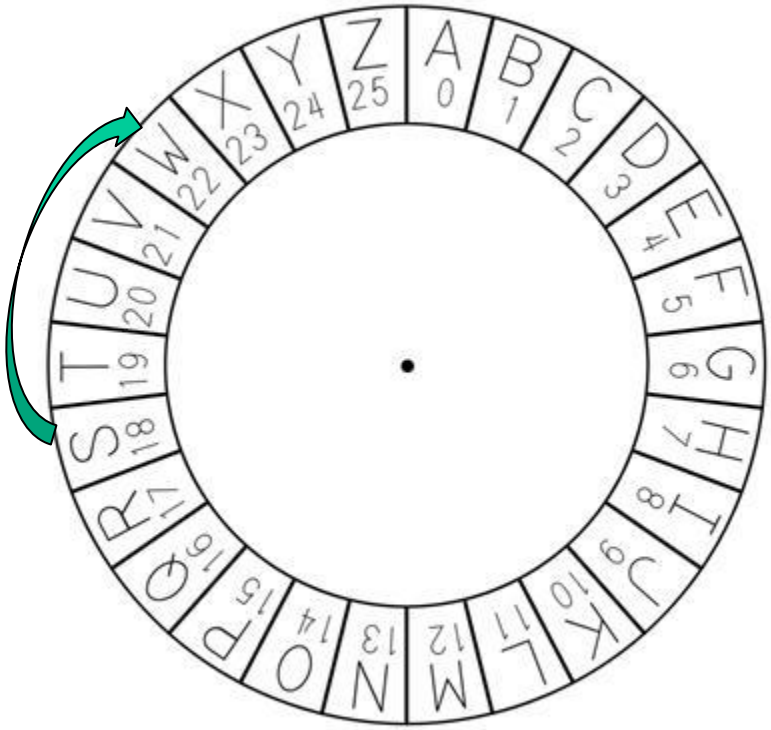
Compose a secret **message**.
Choose a number from 1 to 25 = your **secret key**.
Add your **key** to each **letter of your message**
using **modular arithmetic** (= clock arithmetic).

Example:

```
  S  E  C  R  E  C  Y
+ 4  4  4  4  4  4  4
-------------------
  W  I  G  V  I  G  C
```

the secret key

the cipher-text



To decrypt the ciphertext, we just subtract the secret key.

uOttawa

Your turn

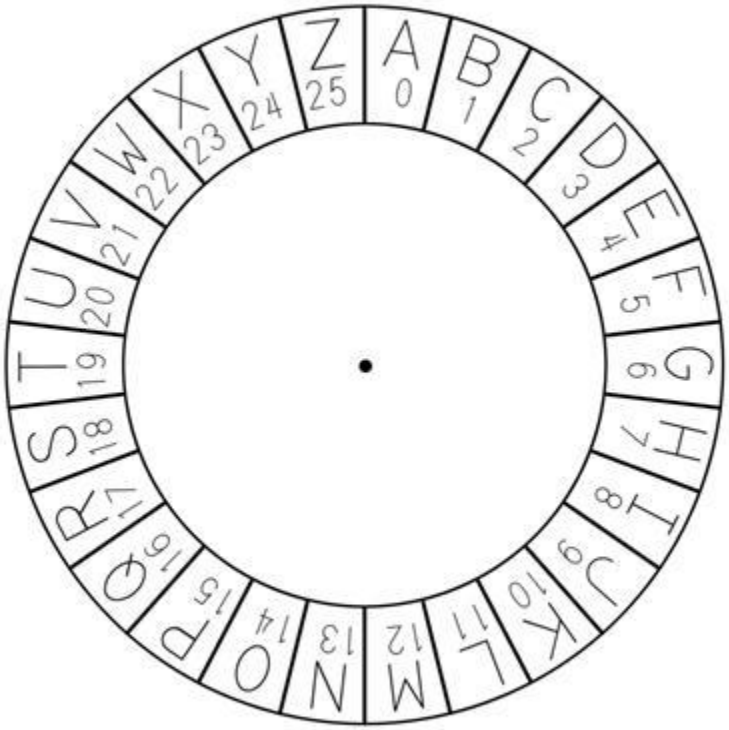
1. Choose a short secret **word**.

2. Choose your **secret key** (a number from 1 to 25)

3. Secretly add your **key** to each **letter of your word.**

4. Pass the ciphertext to Eve/Yves who will give it to your partner.

5. **Tough part:** give your secret key to your partner **without** Eve/Yves (or others) hearing it.



uOttawa

But is the Caesar cipher **good** cryptography?

Not really. It has at least **three big problems**:

1. Just 25 keys – so not hard for Eve to guess and crack the code.
2. Can only encrypt words in 26 letters (and tediously, at that).
3. It's just as hard to share the secret key as it would be to whisper the secret word!

So let's just solve these 3 problems, and we'll get one of the best modern cryptosystems in the world.

Solving problem #1: more keys

Substitution cipher : instead of just shifting the alphabet, choose a permutation of the alphabet, like

Plaintext	A	B	C	D	E	F	G	H	I	…
Ciphertext	M	A	T	H	I	S	F	U	N	…

How many keys are there now?

= 25 x 24 x 23 x 22 x 21 x ….

= 25! ("25-factorial")

= 15,511,210,043,330,985,984,000,000

Better, but not good enough: repeated letters give too many clues (using frequency analysis).

Solving problem #1: Second World War

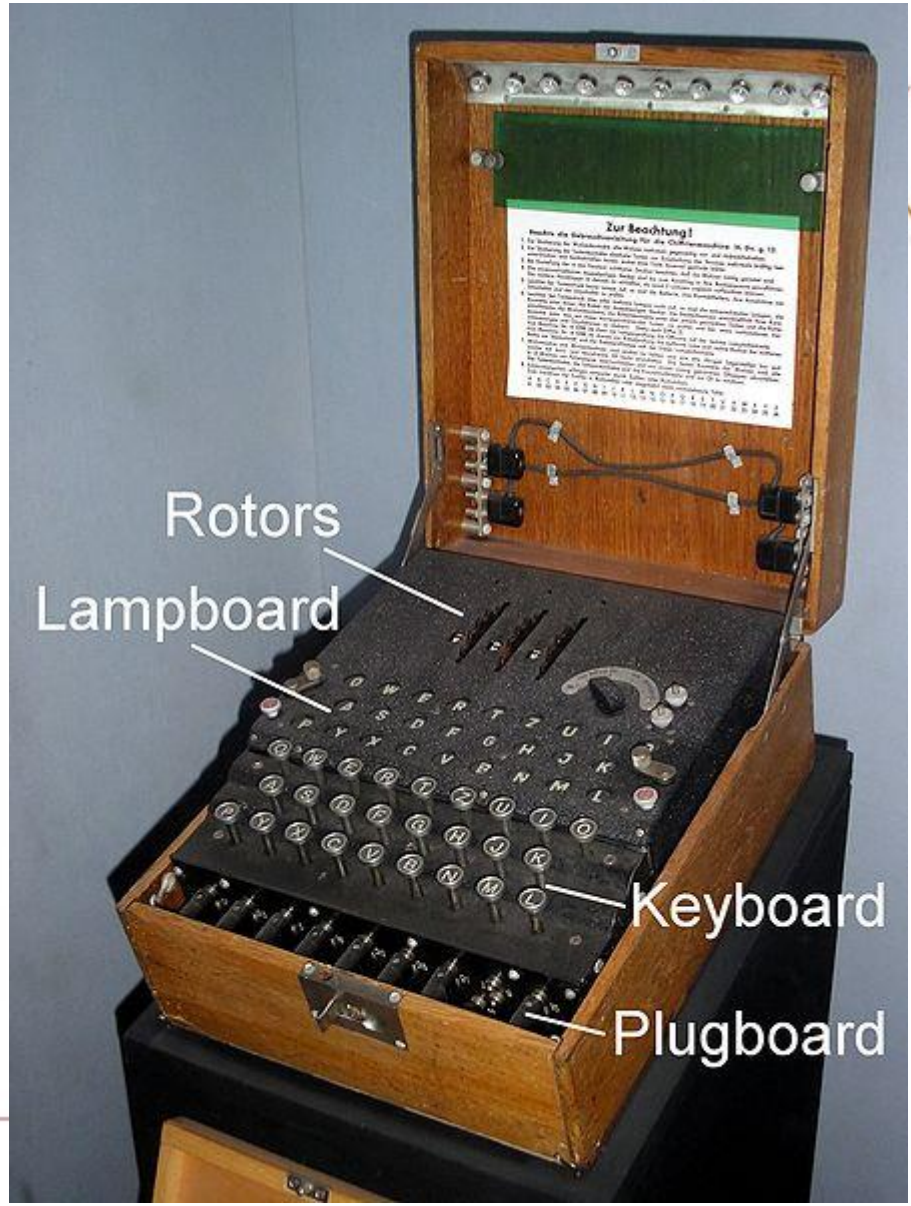
The Germans used the **Enigma machine**

which encrypted each letter to a **different** letter each time, because the rotors turned.

About a sextillion keys, and no patterns in the ciphertexts =

"Completely uncrackable"

Cracked by mathematicians in early 1940.



uOttawa

Solution to problem #1: Perfect secrecy

A **one-time pad** is a random sequence of numbers, like

8	14	9	0	16	23	1

To encrypt a message with a one-time pad, just add them:

	S	E	C	R	E	C	Y
+	8	14	9	0	16	23	1
=	A	S	L	R	U	Z	Z

uOttawa

This is in fact completely uncrackable (i.e. the ciphertext can't be decrypted without the secret key) **IF** you only use the **one-time pad** **once**.

Recall: we're trying to solve 3 problems

1. Just 25 keys – so not hard for Eve to guess and crack the code.

Replace Caesar cipher with one-time pad

2. Can only encrypt words in 26 letters (and tediously, at that).

3. It's just as hard to share the secret key as it would be to whisper the secret word!

Solving problem #2, first step:

Everything is a number, via the ASCII (or UTF-8) code…

Code	Char	Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
32	[space]	48	0	64	@	80	P	96	`	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	"	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	'	55	7	71	G	87	W	103	g	119	w
40	(	56	8	72	H	88	X	104	h	120	x
41	)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[	107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o	127	[backspace]

A portion of the UTF-8 code table

Solving problem #2, continued:

…and every number is a sequence of 0s and 1s

Time for a magic trick.

The secret : Every number can be written in a unique way as a sum of some of the powers of 2.

Power of 2:	32	16	8	4	2	1
Example: 41 =	32 +		8 +			1
	1	0	1	0	0	1

Shorthand : 41 is 101001 in **binary notation**

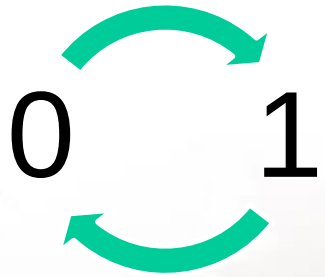
You can use an online ASCII decoder:

http://www.dcode.fr/ascii-code

Solution to problem #2, final step:

Addition *mod 2*

It is easy to do modular arithmetic with binary numbers:



Rules:

0+1=1 0+0=0
1+0=1 1+1=0

Message (in ASCII)	1	0	1	1	0	0	0	(X)
One-time pad (in binary)	1	1	1	0	1	0	1	
Sum mod 2	0	1	0	1	1	0	1	(-)

OK, good progress on 2 of 3 problems:

1. Just 25 keys – so not hard for Eve to guess and crack the code. ✓ Replace Caesar cipher with one-time pad

2. Can only encrypt words in 26 letters (and tediously, at that). ✓ Use ASCII and binary addition

3. It's just as hard to share the secret key as it would be to whisper the secret word!

Solving problem #3: your turn

Goal: devise a means for Alice to send a **secret key** to Bob **even though** Eve can intercept (but not break) everything that Alice gives to Bob.

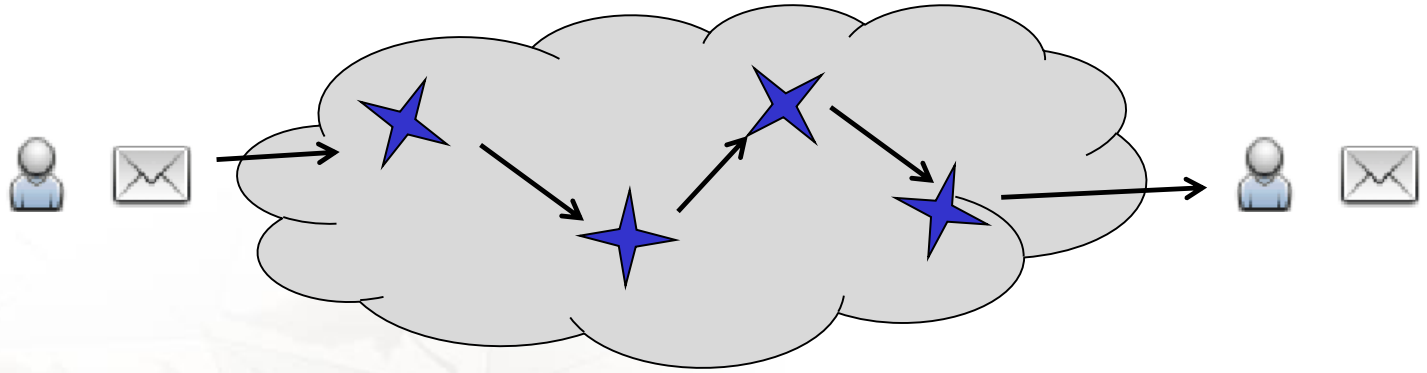
Items: (use some, or all, of them)

Tool box (empty)	Plank
Rope	Light switch
Lightbulb	Refrigerator
Two locks	Elephant
Keys for the locks	Feather

Solving problem #3 = modern (mathematical!) cryptography

Millions of people need private, secure communication.

The internet is open to **every kind** of eavesdropping.



How do we exchange secrets in a completely insecure environment?

Short answer: use **mathematical functions** which are **easy to compute**, but **insanely difficult** to invert: **one-way functions.**

uOttawa

We need 3 mathematical ingredients…

Ingredient A: Prime numbers

A number p>1 is **prime** if its only factorization is p=1xp.

The first primes are

2, 3, 5, 7, 11, 13, 17, 19, …

They are like the **atoms** of multiplication.

- There are ∞ many primes
- With **Number Theory**, they are pretty easy to find
- Humans don't know any pattern in their distribution, or any formula that always gives a prime. They are really incredibly random.

RIEMANN HYPOTHESIS
#1 Millenium Prize Problem ($1,000,000)

uOttawa

Some big prime numbers

15 485 863 is the millionth prime number

Mersenne primes are those which are 1 less than a power of 2.

- The first Mersenne primes are 3, 7, 31, 127.
- 170 141 183 460 469 231 731 687 303 715 884 105 727 is the twelfth Mersenne prime (proven prime in 1876)
- The largest Mersenne prime found so far has 22 million digits.

For cryptography, we just need primes that have at least 300 digits, like:

39,582,032,730,632,272,020,877,348,904,469,924,393,976,541,004,775,366,615,
511,832,138,158,640,305,883,728,172,536,064,352,212,381,908,995,524,757,29
8,930,812,787,042,060,975,659,965,565,129,828,970,355,677,718,000,393,369,4
28,727,749,354,587,613,617,639,268,683,028,155,301,839,520,701,056,817,640,
702,570,125,125,426,571,875,106,377,220,407,795,420,832,613,733,344,908,01
7,898,731,562,573,179,060,464,591,399

https://asecuritysite.com/encryption/random3?val=1024

First example of a one-way function

Multiplication:	Factorization:
$5 \times 7 = 35$	$21 = 3 \times 7$
$7 \times 11 = 77$	$57 = 3 \times 19$
$11 \times 13 = 143$	$91 = 7 \times 13$

Multiplication is **easy** – but factorization is **hard** (even for powerful computers, if the numbers are big enough)

Ingredient B : powers

Eg: $3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 3x3x3 = 27$, $3^4 = 3x3x3x3 = 81$, …

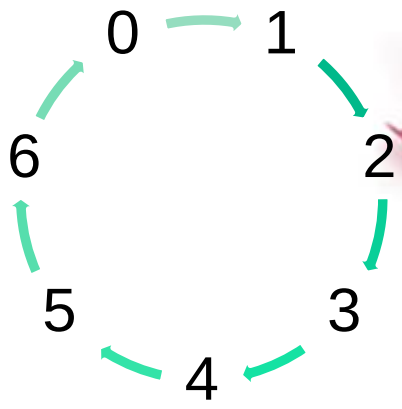
$$3^{20} = \overbrace{\underbrace{(3 \times 3 \times 3 \times 3)}_{4\text{ terms}} \times \underbrace{(3 \times 3 \times 3 \times 3)}_{4\text{ terms}} \times \cdots \times \underbrace{(3 \times 3 \times 3 \times 3)}_{4\text{ terms}}}^{5\text{ groups}}$$

$$= (3^4)^5$$
$$= (3^5)^4$$

(The answer is HUGE: 3,486,784,401.)

uOttawa

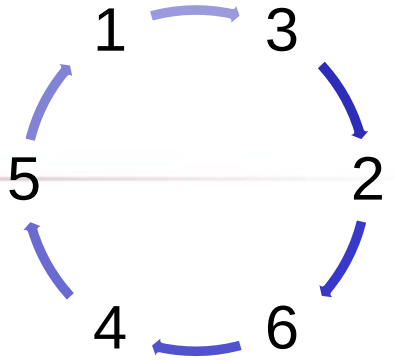
Ingredient C : powers mod p (p=7)



n	3^n	$[3^n]_7$ = remainder when you divide 3^n by 7
0	1	1
1	3	3
2	9	2
3	27	6
4	81	4
5	243	5
6	729	1
7	2187	3
…	…	…

Tip: Instead of calculating 3^n and then dividing by 7, just multiply each line by 3 to get the next line.

The answers give a new RANDOM cycle:



Cool fact: this is another one-way function (if p is really BIG)

uOttawa

Your turn: powers mod 11

Fill in the table of powers of 2 "mod 11" until you get a cycle:

n	2^n	$[2^n]_{11}$ = remainder when you divide 2^n by 11
0	1	1
1	2	2
2	4	4
3	8	8
4	16	
5	32	
6	64	
…	…	…

uOttawa

Back to cryptography:

Now let's assemble the ingredients, and create a secret key in full view of Eve:

Alice Bob Eve

Diffie and Hellman's idea (1978)

Let's take p=11, and base 2.

5

6

I'll secretly pick a=4.
So $[2^4]_{11}$= **5.**

I'll secretly pick b=9.
So $[2^9]_{11}$= **6.**

Shared secret key

Alice calculates:
$[6^4]_{11}$= **9**

$2^{36} = (2^9)^4$

$2^{36} = (2^4)^9$

Bob calculates:
$[5^9]_{11}$= **9**

???

$2^{36} \neq (2^4)(2^9)$

uOttawa

Your turn: sharing a secret one-time pad with a partner

- Choose together a prime number **p** (like 47) and a base **x** (like 2 or 3).
- Choose your own secret number **a** (like 7); don't share it.
- Calculate $\mathbf{[x^a]_p}$ using a modular exponentiation calculator like

http://www.dcode.fr/modular-exponentiation-calculus

- Write down the answer (**A**) and pass it to Eve/Yves. Eve/Yves can't figure out **a** (if you chose **p** large enough!).
- When Eve/Yves gives you your partner's answer (**B**), take it to your secret power **a** (mod **p**). Call your answer **K**.
- No matter what secret number your partner picked, you will both get the same answer **K** – so this is your shared secret key! (And Eve/Yves saw it all, but has nothing.)

Caesar cipher to Diffie-Hellman, and beyond…

1. Just 25 keys – so not hard for Eve to guess and crack the code.

   Replace Caesar cipher with one-time pad

2. Can only encrypt words in 26 letters (and tediously, at that).

   Use ASCII and binary addition

3. It's just as hard to share the secret key as it would be to whisper the secret word!

   Use the Diffie-Hellman key exchange

Problem solved… or is it?

Diffie-Hellman is very secure – as long as the prime p is so big that searching for your secret exponent would take Eve longer than the age of the universe to do.

The encryption on your internet browser is based on Diffie-Hellman and on similar schemes, like RSA, and it is perfectly secure.

Except…

We now know that a

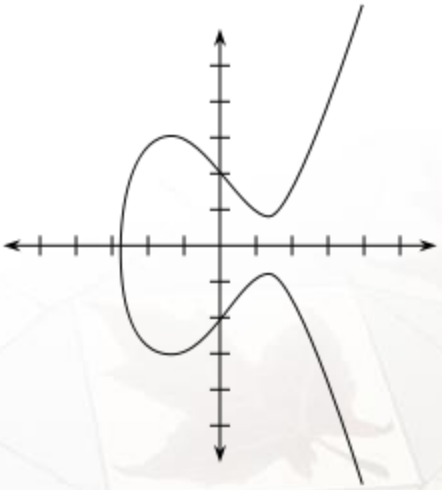
Quantum computer

Could crack RSA and Diffie-Hellman…

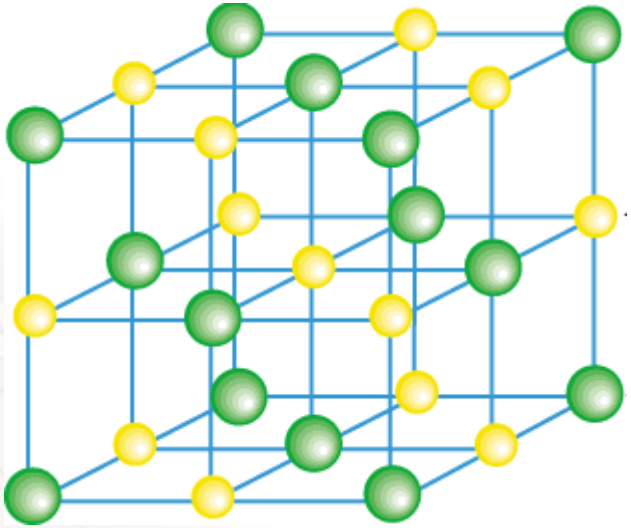
uOttawa

Where to next?

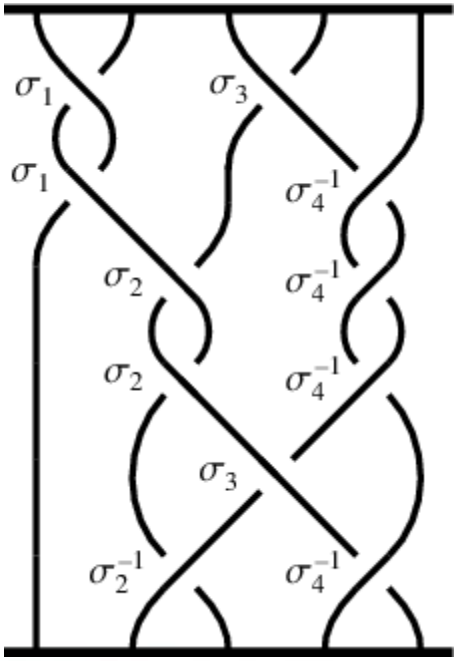
RSA & Diffie-Hellman are just some of the many mathematical cryptosystems in development today. There is no lack of cool **mathematical problems** to use, from such varied sources as:



Elliptic curves



Lattices (systems like NTRU)



Braid groups

uOttawa

Further reading

Cryptography:

Simon Singh, The Code Book
Available on-line, with applications

Number Theory:

James Tattersall
Elementary Number Theory in Nine Chapters

Questions?

mnevins@uottawa.ca

uOttawa