Prime Numbers and Cryptography (1)

- Today, many modern cryptosystems are designed using **Modular Arithmetic** and **prime numbers**.
- Why are Modular Arithmetic and prime numbers are useful for cryptography?
- Calculation in Modular Arithmetic looks random. But it has beautiful laws.

Prime Numbers and Cryptography (2)

- **Weakness of Caesar cipher**

  shifts A→D, B→E, C→F ⋯ are too simple operations.

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

ILOVEPRIMENUMBER → LORYHSULPHQXPEHU

Prime Numbers and Cryptography (3)

- **Operations in Modular Arithmetic**

A\B	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

$A + B \pmod 5$

A\B	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

$A \times B \pmod 5$

- **Addition**: too simple
- **Multiplication**: we can calculate inverses.

Prime Numbers and Cryptography (4)

- **Exponentiation** seems **complicated**.

K	1	2	3	4	5	6	7	8	9	10
$2^K \pmod{11}$	2	4	8	5	10	9	7	3	6	1
$6^K \pmod{11}$	6	3	7	9	10	5	8	4	2	1
$7^K \pmod{11}$	7	5	2	3	10	4	6	9	8	1

- By **Fermat's Little Thm**,

$$A^{10} \equiv 1,\ \ A^5 \equiv -1 \equiv 10 \pmod{11}$$

- Apart from them, we do not see any simple patterns.

Prime Numbers and Cryptography (5)

Problem Assume $A^K \equiv B \pmod{N}$.

(1) (**Discrete Logarithm Problem**)

If we know A,B,N, can we calculate K?

(2) If we know K,B,N, can we calculate A?

- No efficient algorithms are known.
- Many modern cryptosystems are based on the hardness of them (or their variants).

Prime Numbers and Cryptography (6)

- Many modern (Public Key) Cryptosystems are designed using prime numbers.
- The security of them is **not** proved.
- People believe they are probably secure because
  - known attacks require to solve **Discrete Logarithm** or **Integer Factorization Problems**, and
  - these problems seem difficult to solve.

Interlude: Quantum Computers

- In 1994, Shor discovered efficient algorithms to solve Discrete Logarithm and Integer Factorization Problems on a **quantum computer**.
- In the future, when quantum computers become available, will cryptosystems be broken by quantum computers?

Peter Shor
(1959-)

http://www-math.mit.edu/~shor/