2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

More Fun with Prime Numbers

Week 4

Prime Numbers and Cryptography

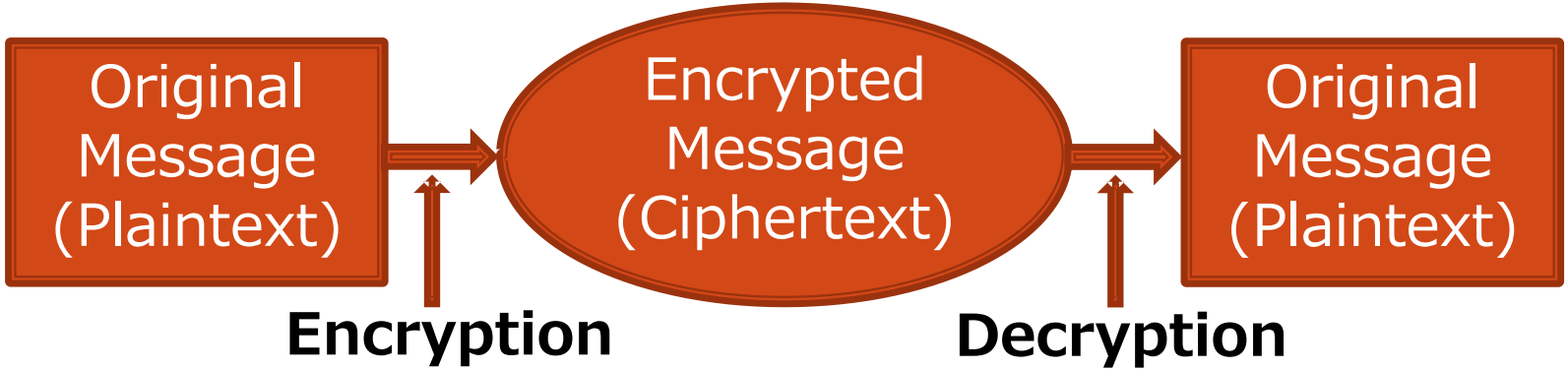
Tetsushi Ito

Department of Mathematics
Kyoto University

What is Cryptography? (1)

- Recently, prime numbers are applied to construct practical cryptosystems.
- Secure electronic communication is not possible without using prime numbers!

What is Cryptography? (2)



- We encrypt/decrypt message using keys.
- It should be very difficult to recover the plaintext from the ciphertext without the decryption key.

What is Cryptography? (3)

Example (Caesar cipher)

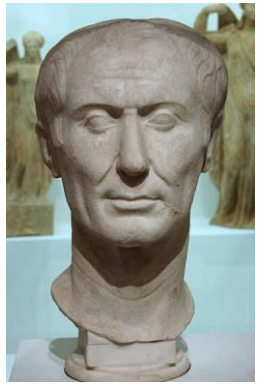
A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	O	P

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

Encryption Key +3

Decryption Key −3



Gaius Julius Caesar (100BC-44BC)

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

What is Cryptography? (4)

- **Caesar cipher** is simple and fast.
- But, it is not secure. One can calculate encryption/decryption keys once a plaintext-ciphertext pair was revealed.
- How can we design more secure cryptosystems?
- **Caesar cipher is symmetric**:
  (Encryption Key) = (−1)×(Decryption Key)