The World of Algebra
—Number Theory and Its Application—

#2 Digital Mathematics, Mathematics for Security
—Cryptographic theory—

Graduate School of Mathematical Sciences,
the University of Tokyo

Toshiyuki Katsura

1. Cryptograph

cryptograph

Special code made to communicate secretly, which can be interpreted only by the parties involved.

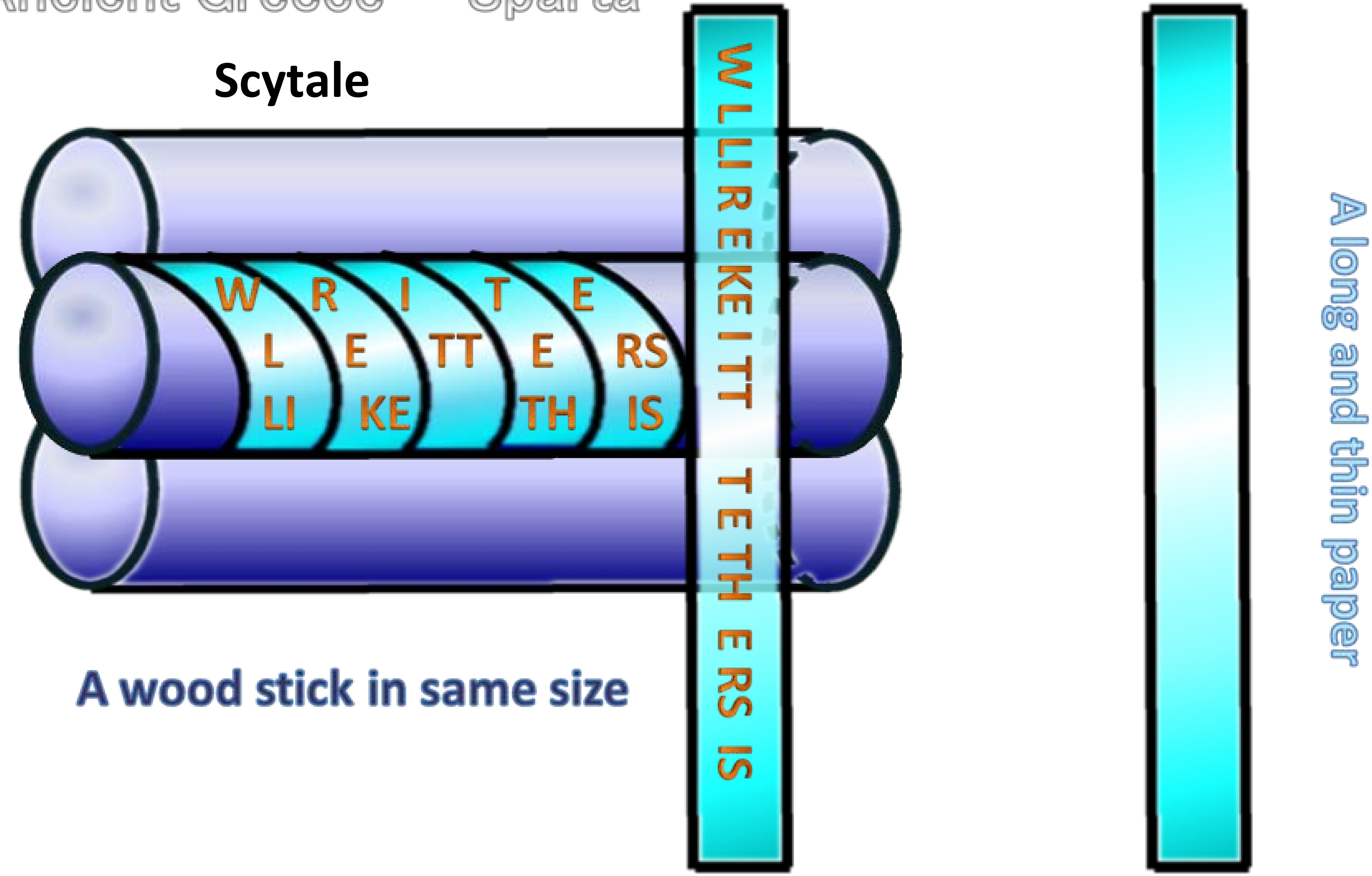
Or to make changes in sentences transmitted in a special way.

Here, the latter is dealt with.

Plain text	**Sentence to be transmitted**
Cryptograph	Changed sentence
Cipher	A **tool to decode cryptograph back into plain text**

Ancient Greece Sparta

Scytale



Twist a long and thin paper around a stick, and write letters on it along the stick

Caesar Cipher

Each letter is replaced by a letter some fixed number of positions further down the alphabet.

Ex. shift of 1

plain	HUKANKOUGI
cryptograph	IVLBOLPVHJ
cipher	shift of 1

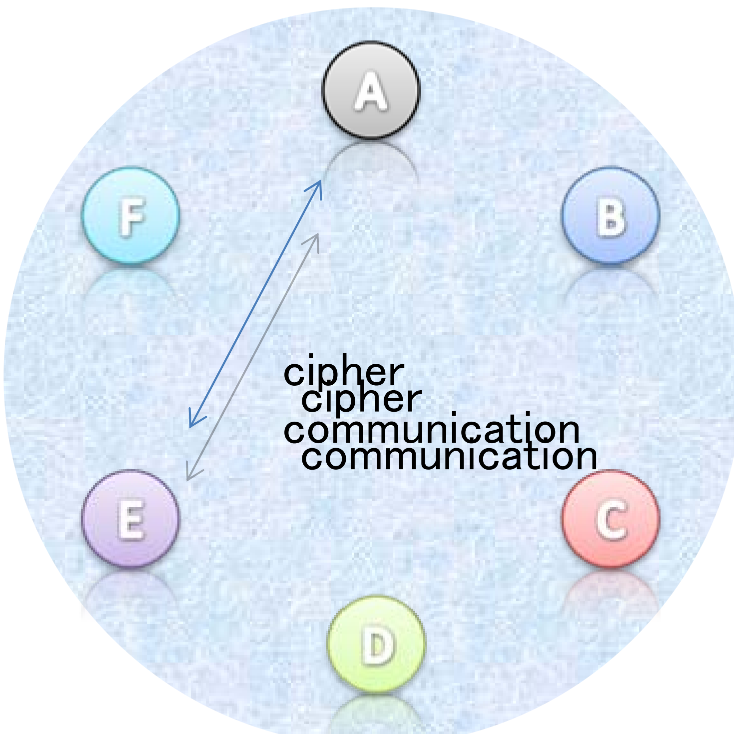
Symmetric-Key Cryptography

A cryptography whose cipher is shared by sender and receiver.

1976 W. Diffie, M.Hellman

It was discovered that cipher communication between two unspecified people is possible even when a cipher is open to general public.

Public-key cryptography



Key is widely distributed.

The Principle of Public-Key Cryptography

Even the quickest computer takes an inordinate amount of time to solve its algorithm, decoding is practically impossible.

Organic law

(1) By a difficult prime-factor-decomposed computation

(2) By a difficult discrete logarithm problem

RSA cryptography using (1)is to be introduced.

2. Theorems of Number Theory

theorem (Fermat's little theorem)

if p is a prime number and a is any integer that does not have p as a factor,

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

proof

Let us assume that $\{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ **is a member of** $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ **not including** $\overline{0}$

Since a **is not divisible by** p **,**

$$\{\overline{1}, \overline{2}, \cdots, \overline{p-1}\} = \{\overline{a} \cdot \overline{1}, \overline{a} \cdot \overline{2}, \cdots, \overline{a} \cdot \overline{p-1}\}$$

therefore,

$$\begin{aligned} \overline{1} \cdot \overline{2} \cdot \ \cdots \ \cdot \overline{p-1} &= \overline{a}\,\overline{1} \cdot \overline{a}\,\overline{2} \cdot \ \cdots \ \cdot \overline{a}\,\overline{p-1} \\ &= \overline{a}^{p-1} \cdot \overline{1} \cdot \overline{2} \cdot \ \cdots \ \cdot \overline{p-1} \end{aligned}$$

$\overline{1} \cdot \overline{2} \cdot \ \cdots \ \cdot \overline{p-1}$ **is** $\mathbb{F}_p$ **and not** $\overline{0}$

$$\overline{a}^{p-1} = \overline{1}$$

Ex. 1

$p = 71$ **prime**

$a = 1687$ **is not divisible by** p.

$$1687^{70} \equiv 1 \pmod{71}$$

Ex. 2

$q = 97$ **prime**

$a = 1687$ **is not divisible by** q.

$$1687^{96} \equiv 1 \pmod{97}$$

Generalize Fermat's Little Theorem Slightly, and Use it in a Code.

p, q 2 prime numbers

$\mathbb{Z}/pq\mathbb{Z}$ commutative ring

theorem

If a **is an integer coprime to** pq **, then**

$$a^{(p-1)(q-1)} \equiv 1 (\text{mod } pq)$$

example

Suppose $p = 71, q = 97, pq = 6887$

Then

$$(p-1)(q-1) = 6720$$

$a = 1687$ **cannot be divided by** p, q

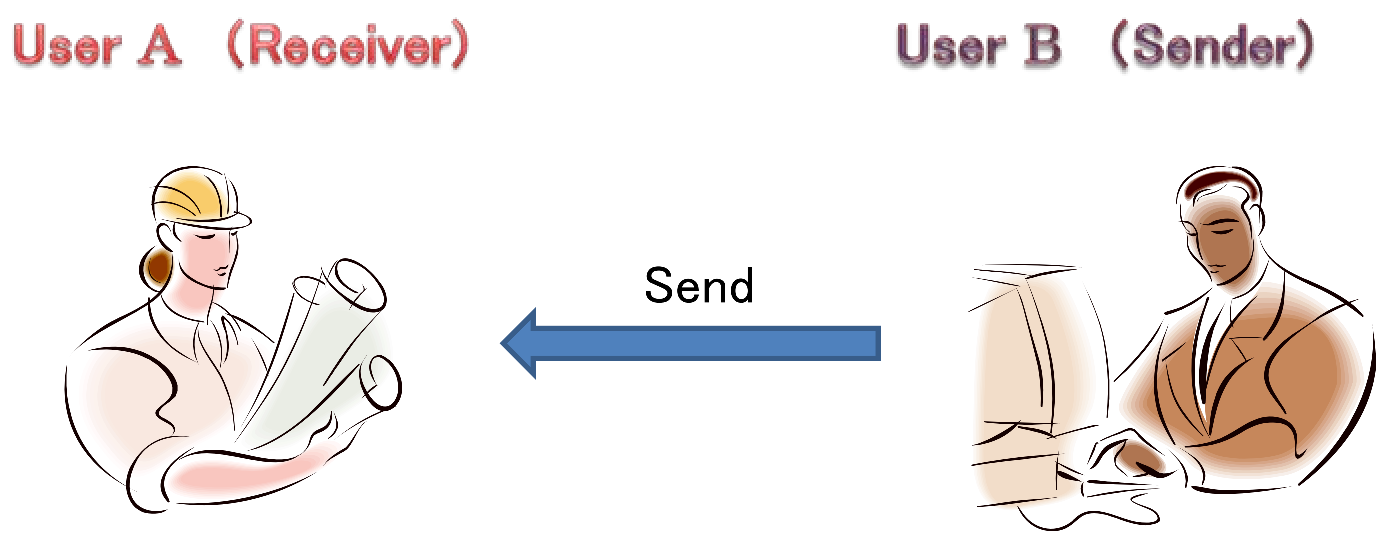
$$1687^{6720} \equiv 1 \ (\text{mod } 6887)$$

3. RSA public key encryption

1978

Presented by R.Rivest, A.Shamir, L.N.Adleman

- Public key cryptography using the fact that it is difficult to factorize product of 2 large prime numbers.



User A（Receiver）

Selects 2 large primes, p, q

and compute $n = pq$

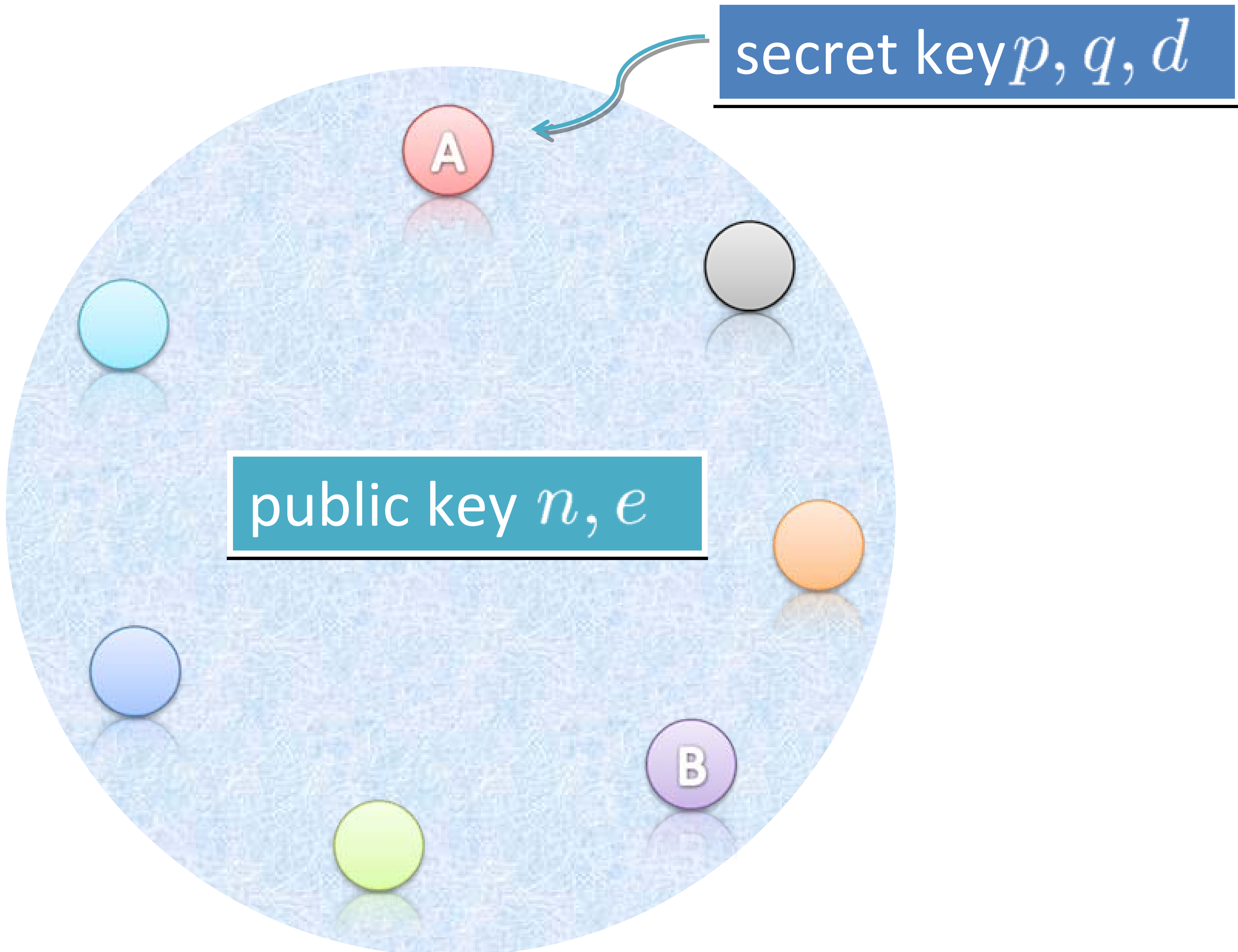
Chooses an integer $\overline{e}$ from $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$

such that an integer d exists when

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

public key n, e

secret key p, q, d



secret key p, q, d
A
public key n, e
B

User B (Sender)

Send a plain sentence M which is coprime to n .

encryption M^e

principl
e

Third person cannot calculate d since prime factorization of n is extremely difficult.

User A (Receiver)

reconstruct M from $(M^e)^d \equiv M \pmod{n}$

Verification

From generalization of Fermat's little theorem,

$$M^{(p-1)(q-1)} \equiv 1 \pmod{n}$$

Since $ed \equiv 1 \pmod{(p-1)(q-1)}$**, there is an integer** s

$$ed = (p-1)(q-1)s + 1$$

Therefore,

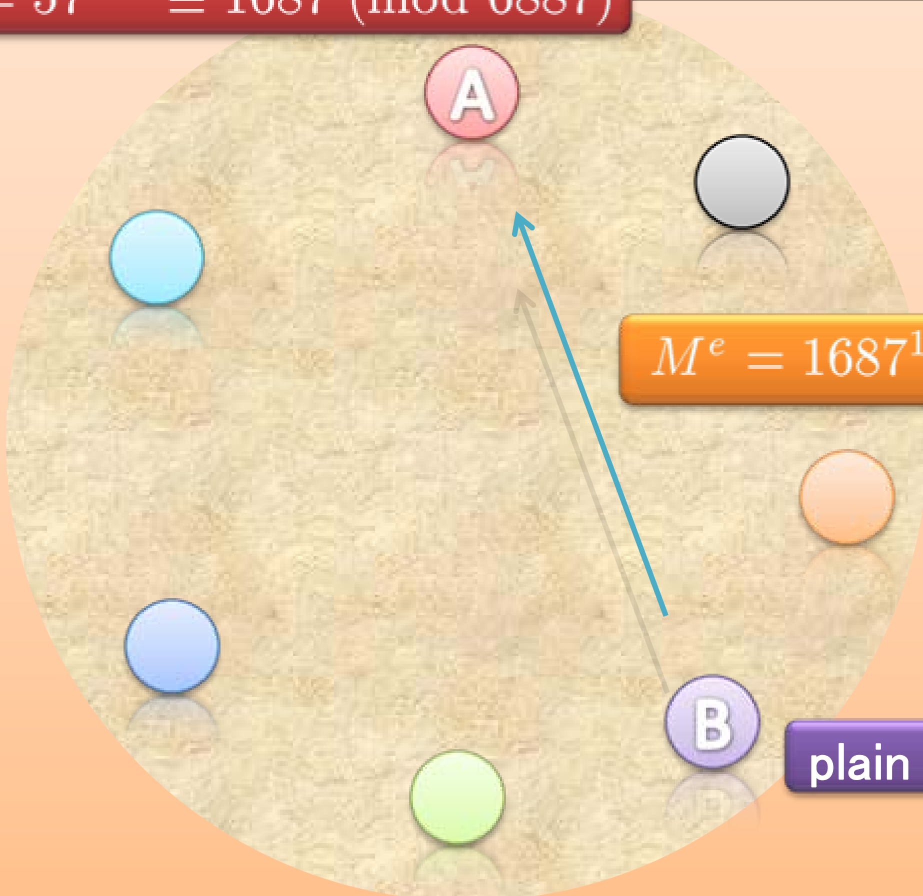
$$\begin{aligned} M^{ed} \pmod{n} &\equiv M^{(p-1)(q-1)s+1} \pmod{n} \\ &\equiv (M^{(p-1)(q-1)})^{s} M \pmod{n} \\ &\equiv M \pmod{n} \end{aligned}$$

Example

secret key: $p = 71, q = 97, d = 517$

public key : $n = pq = 6887, e = 13$

$57^d = 57^{517} \equiv 1687 \pmod{6887}$



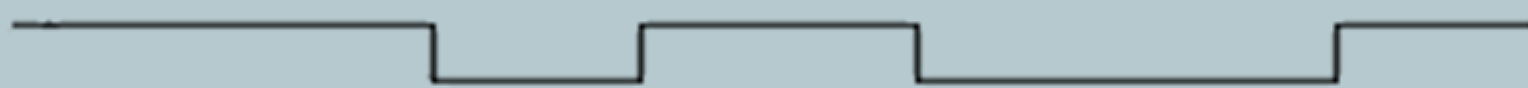
$M^e = 1687^{13} \equiv 57 \pmod{6887}$

plain sentence $M = 1687$

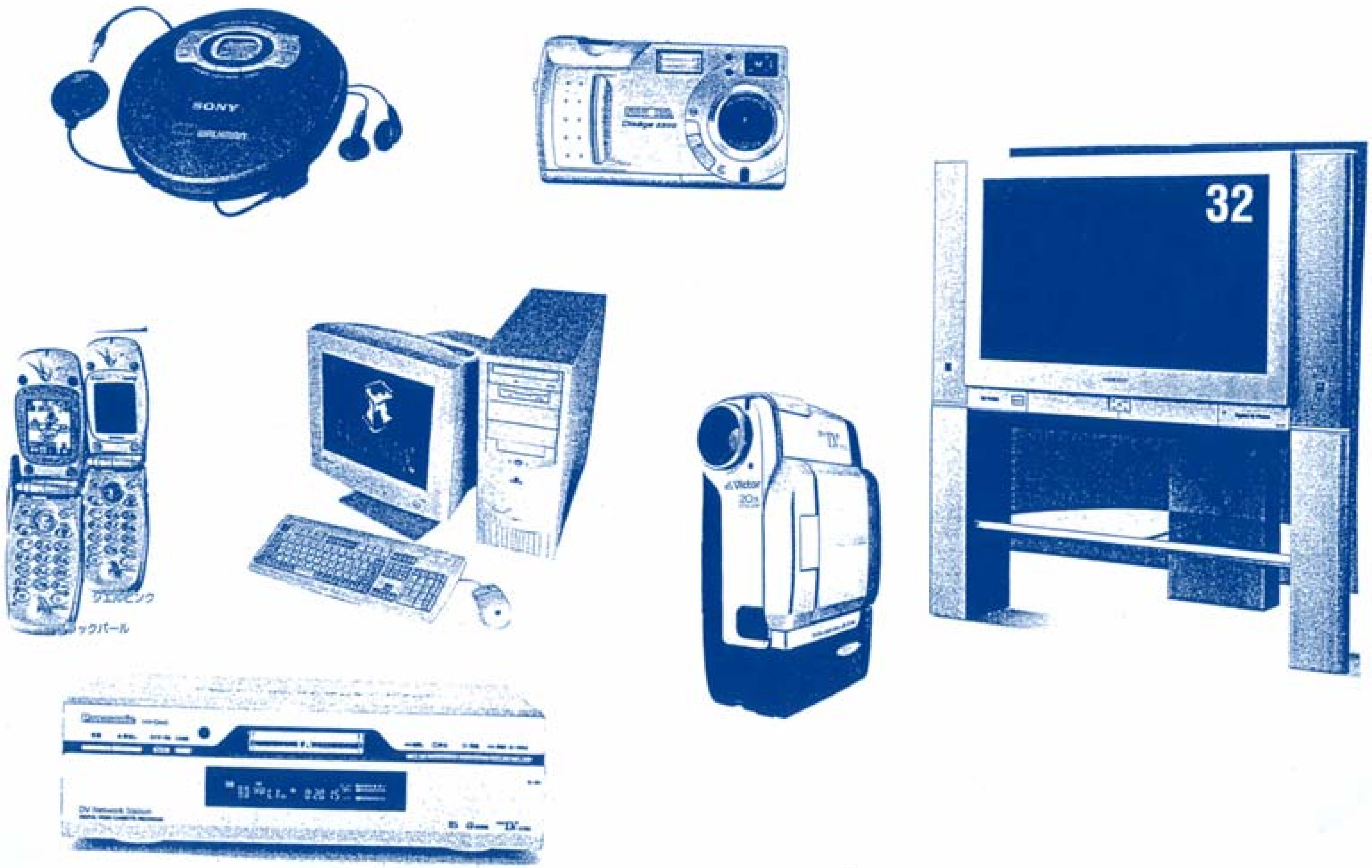
4. Code Theory

Analog to Digital

Compact Disc



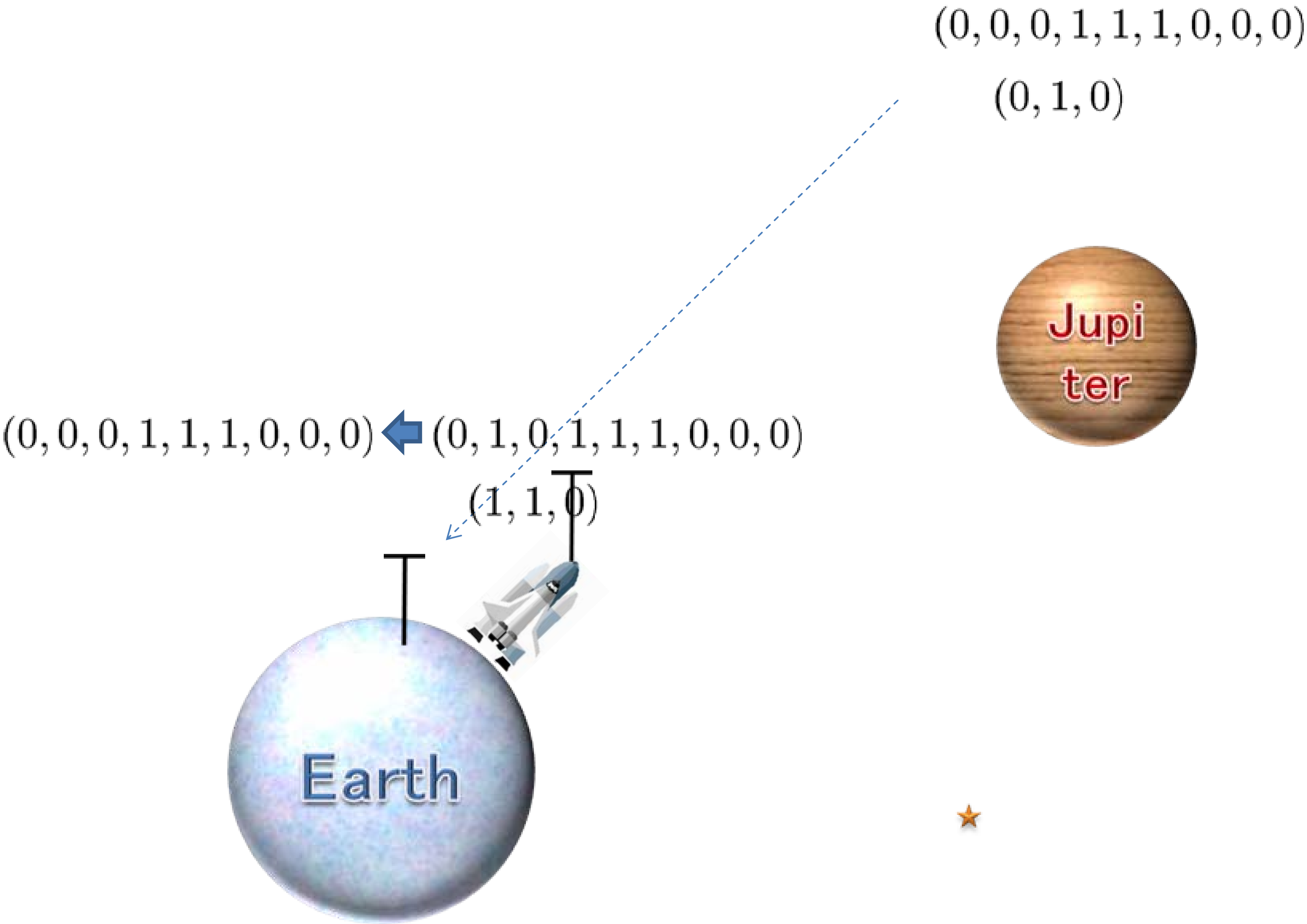
0 0 0 0 0 1 0 0 1 0 0 0 1 0 0 0 0 0 1 0 0


SONY
ジェルピンク
Victor
32
DV Network Station

Where Digital is, Error Exists

Error-correction code

Error-detection code



$(0,0,0,1,1,1,0,0,0)$
$(0,1,0)$
Jupi
ter
$(0,0,0,1,1,1,0,0,0)$
$(0,1,0,1,1,1,0,0,0)$
$(1,1,0)$
Earth


Information source
coder
Transmission channel
decoder
destination

$\mathbb{F}_q^n$: n -dimensional vector space in $\mathbb{F}_q$.
$(x_1, x_2, \cdots, x_n)$ are called **alphabets**.

$\mathbb{F}_q^n \supset C$
C is called **code**.
Members of C are used as alphabets.
n : word length of C .

$\mathbb{F}_q^n \setminus C$: redundancy
This is used for error-correction.

The larger C is, the more information can be transmitted.

Ability of error-correction is generally higher if $\mathbb{F}_q^n \setminus C$ is larger.

More efficient code that fulfills both of these conflicting conditions is desired.

Distance of $\mathbb{F}_q^n$ is Defined to Check Errors.

Distance

A distance between 2 points $P = (x_1, x_2, x_3)$ **and** $Q = (y_1, y_2, y_3)$ **in 3-dimensional Euclidean space** $\mathbb{R}^3$

$$d(P, Q) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2}$$

that fulfills 3 conditions below.

(i) $d(x, y) \geq 0.$ or $d(x, y) = 0 \Leftrightarrow x = y.$

(ii) $d(x, y) = d(y, x)$

(iii) [triangle inequaity] $d(x, y) + d(y, z) \geq d(x, z)$

These 3 conditions are essential for distance.

In other words, if these 3 conditions are fulfilled, it can be called a distance.

Definition

distance of $\mathbb{F}_q^n \ni x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n)$

(Hamming distance)

$$d(x, y) = \sharp\{1 \leq i \leq n \mid x_i \neq y_i\}$$

Here, $\sharp S$ **is a number of members in group** S **.**

That this fulfills the axiom of distance space can be easily verified.

For example, in $\mathbb{F}_2^5$ **, 4 components are different in** $x = (1, 0, 1, 0, 1)$ **and** $y = (1, 1, 0, 1, 0)$ **, so** $d(x, y) = 4$ **.**

In other words, if $x = (1, 0, 1, 0, 1)$ **is sent and** $y = (1, 1, 0, 1, 0)$ **is received, error with Hamming distance of** $d(x, y) = 4$ **has occurred.**

Definition

When $z \in \mathbb{F}_q^n$, and r is a natural number.

$$B_r(z) = \{x \in \mathbb{F}_q^n \mid d(z,x) \leq r\}$$

is a sphere with a radius r from the center z .

definition

minimal distance d

When C is a subset of $\mathbb{F}_q^n$, its minimal distance d is defined as :

$$d = \min\{d(x,y) \mid x, y \in C,\ x \neq y\}$$

Here, $\min$ stands for minimum value.

Ex.

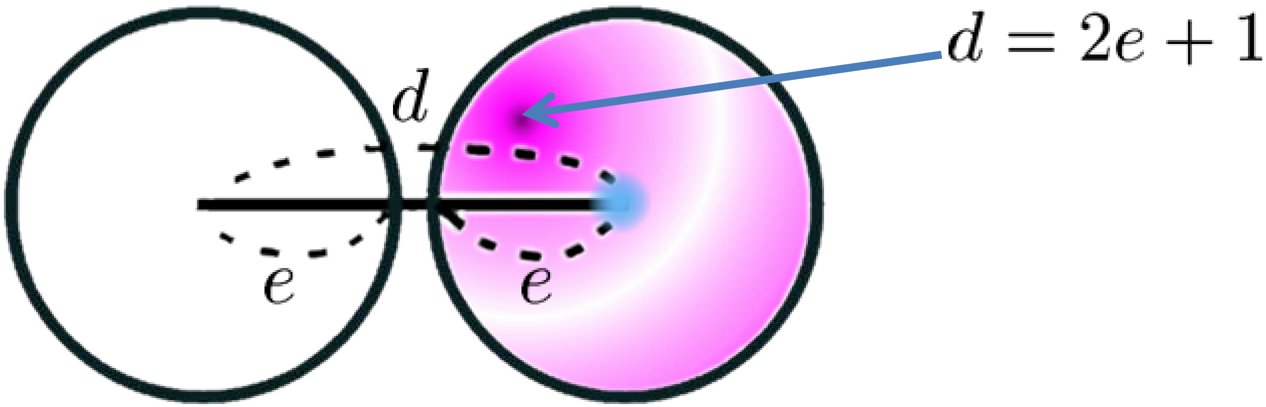
When $\mathbb{F}_2^2 \supset C = \{(0,0),(1,1)\}$

minimal distance $d = 2$

The Principle of Error-Correction

To make it easier to understand,

Suppose a sphere with radius e with a member of C in the center, there is no intersection.



When received code enters into one of those spheres, the closest member of C in the center of that sphere is decoded as a sent code.

maximum-likelihood decoding

- Stochastically, e errors can be corrected.
- ★ When d is an even number, $(d-2)/2$ errors can be corrected.

Question $\mathbb{F}_q^n \supset C$

Construct a subset C of which a Hamming distance between 2 arbitrary points in C is most far.

Hamming code, BCH code, RS code, Golay code, ・・・・