

# 換字(かえじ)暗号

**シーザー暗号**: 各文字をアルファベット上で  **$k$ 字シフト換字** ( $k$  字先の文字に換えること)して暗号を作る暗号方式のこと.

例)  $k = 3$  英小文字だけを対象とする

Good	bye !	a	b	c	d	e	f	g	h	...	w	x	y	z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	...	↓	↓	↓	↓
Grrg	ebh !	d	e	f	g	h	i	j	...	z	a	b	c	

暗号解読

- 頻度配列を使う. eが英文に最も頻繁に現れる

鍵の種類: 26個

⇒ 実は, 復号を26回試せば, 平文が得られる

# 換字(かえじ)暗号

## アルファベット順でない換字

Hellow !	a	b	c	d	e	f	g	h	...	w	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓	...	↓	↓	↓	↓
Hdjjoy!	m	i	n	a	d	e	b	c	...				



この表が鍵

鍵の種類: 26! 個

⇒ 全てを試すのは非現実的

暗号解読

- 頻度配列を使う暗号解読ができる

# 換字(かえじ)暗号

## 周期換字暗号: 変換規則が周期的に切り替わる

例) シーザー暗号を元にした周期換字

$$k_1 = 3, k_2 = 5$$

$i$  番目の文字を  $k_1 + i \times k_2$  字シフト換字

鍵の種類:  $26 \times 26$ 個

暗号解読

- $26 \times i$  番目の文字だけ考える

$$(k_1 + 26 \times i \times k_2) \% 26 = k_1$$

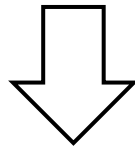
- $i$  番目と  $i+1$  番目の文字を考える

# 転置暗号

## 転置暗号: 文字の位置を置き換える

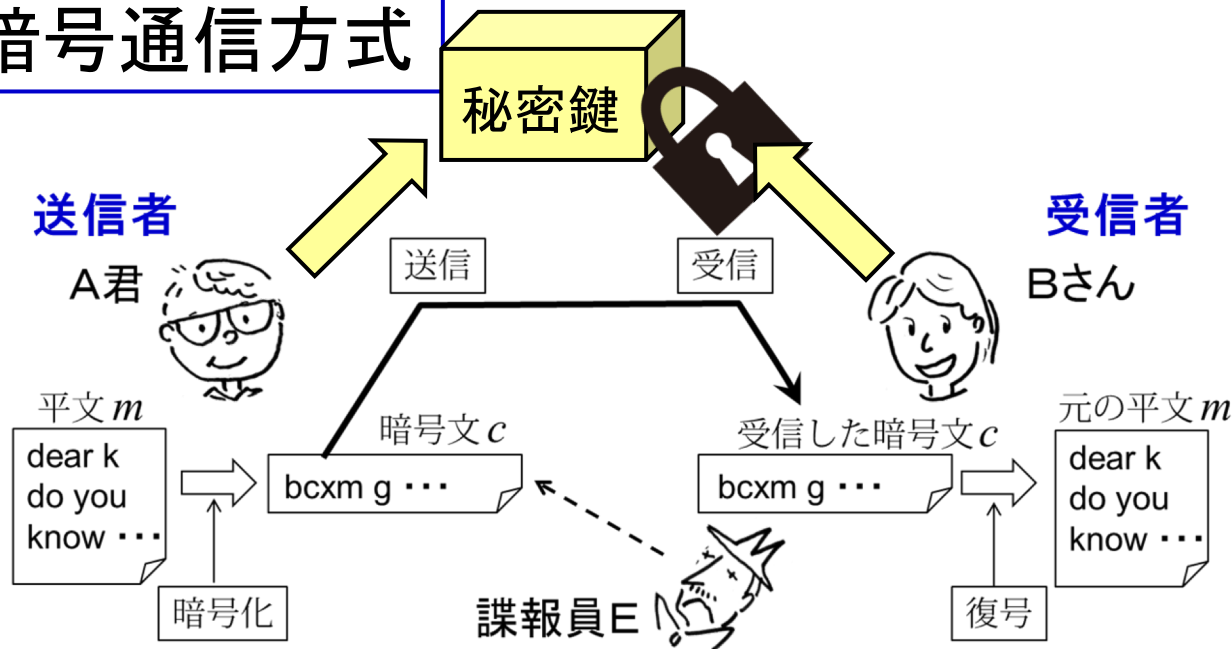
例) 各行を10文字にして, 左から縦に読む

0123456789  
Tokyo Inst  
itute of T  
echnology



Tieotckuhytnoeo lloonfgs y tT

## 4. 現代の暗号通信方式



### 暗号方式の進化

シーザー暗号：ローマ皇帝シーザーが使ったと言われる方式

エニグマ：第二次世界大戦時にドイツ軍が使った方式

DES, AES：現在使われている代表的な暗号方式

1980 年頃

秘密鍵暗号方式

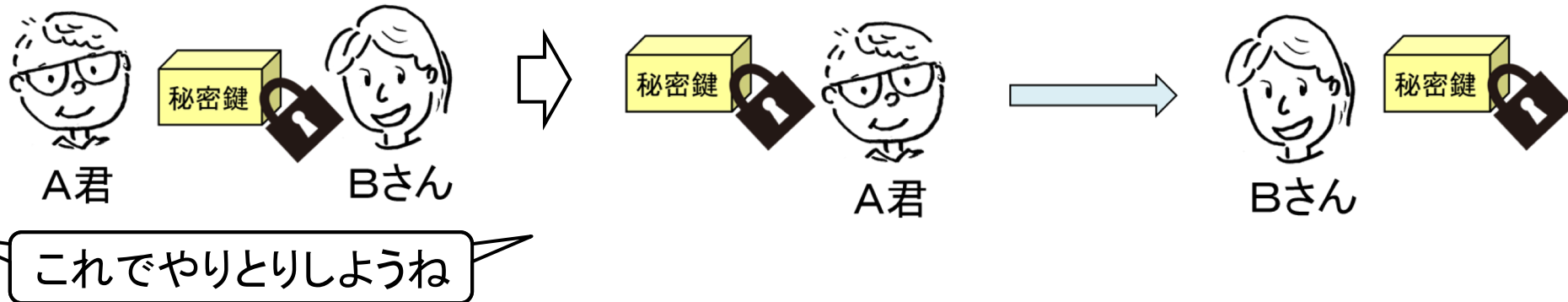
公開鍵暗号方式

公開鍵・・・皆に知らせてよい鍵, 暗号化に使う

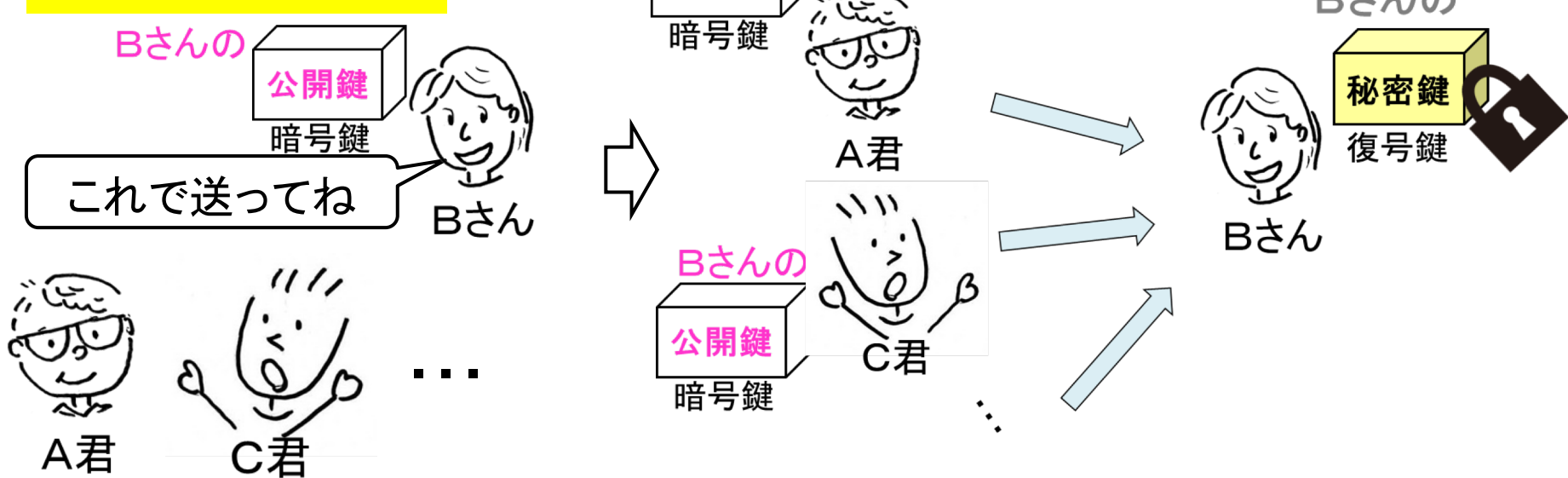
秘密鍵・・・復号に使う

## 4. 現代の暗号通信方式

### 秘密鍵暗号方式



### 公開鍵暗号方式



## RSA暗号(1977年)

RSA(Rivest-Shamir-Adleman)暗号

剰余演算, 特に, フェルマーの小定理が基礎

### フェルマーの小定理

$p$  は素数,  $p$  と  $a$  は互いに素

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

# 剰余演算の復習

## 分配則

$$(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$ab \bmod n = ((a \bmod n) \times (b \bmod n)) \bmod n$$

$$a^k \bmod n = (a \bmod n)^k \bmod n$$

## 記法

$$a = b \pmod{n}$$

$\Leftrightarrow$

$$a \bmod n = b \bmod n$$



# RSA暗号: 鍵生成

1. 大きい素数  $p$  と  $q$  ( $p \neq q$ ) を選ぶ
2.  $n = pq$
3. 暗号化用の鍵  $e$  を  $(p - 1)(q - 1)$  と互いに素になるように選ぶ
4. ユークリッドの互除法で, 以下の等式を満たす 復号用の鍵  $d$  を求める
$$ed = 1 \bmod (p - 1)(q - 1)$$
5. 公開鍵:  $e$  と  $n$   
秘密鍵:  $d$

# RSA暗号:暗号化と復号

## 暗号化

1. 平文を  $n$  より小さいブロックに分ける
2. 一つのブロックを  $m$  とする
3. 暗号文のブロック  $c$  を下の式で計算

$$c = m^e \bmod n$$

## 復号

$$m = c^d \bmod n$$

## 例: RSA暗号

1. 素数:  $p = 3, q = 17, n = pq = 51$
2.  $(p - 1)(q - 1) = 2 \times 16 = 32$
3.  $e = 13$  とする
4.  $13 \times 5 = 1 \pmod{32}$
5.  $d = 5$

## 問題

- 整数 2 を暗号化せよ
- 暗号化した数を復号すると 2 に戻ることを確認せよ

# RSA暗号の公開鍵を見よう！

1. ウェブブラウザで  
<https://www.yahoo.co.jp/>  
を開く
2. 鍵のマークが暗号を使っていることを表している.
3. 鍵をクリック
4. 証明書をクリック
5. 詳細な情報をクリック

## 公開鍵情報

---

アルゴリズム	RSA暗号化 (1.2.840.113549.1.1.1)
パラメータ	なし
公開鍵	256バイト: AD 5D D5 37 E3 19 FF 92 ...
指数	65537
鍵のサイズ	2,048ビット
鍵用途	暗号化, 検証, ラップ, 派生

## RSA暗号：正当性

暗号化  $c = m^e \bmod n$

復号  $m' = c^d \bmod n$

公開鍵で暗号化し，秘密鍵で復号すると元に戻る

正当性：  $m' = m$

$m'$  を計算すると

$$\begin{aligned} m' &= c^d \bmod n \\ &= (m^e \bmod n)^d \bmod n \\ &= m^{ed} \bmod n \end{aligned}$$

よって以下を示す

$$m^{ed} = m \pmod{n}$$

## $m^{ed} = m \pmod{n}$ の証明

$$\begin{aligned} m^{ed} &= m^{k(p-1)(q-1)+1} && \because ed = 1 \pmod{(p-1)(q-1)} \\ &= m \left( m^{(p-1)} \right)^{k(q-1)} && \text{赤の部分にフェルマーの小定理} \\ &= m \pmod{p} \end{aligned}$$

同様にして

$$m^{ed} = m \pmod{q}$$

よって

$$m^{ed} = m \pmod{pq} = m \pmod{n}$$

# RSA暗号：なぜ安全と考えられているか？

公開鍵：  $e$  と  $n$

$n$  を素因数分解できると

⇒  $p, q$  が分かってしまう

⇒ 解読できる

なぜ安全と考えられているか？

「大きな整数の素因数分解が難しい」と考えられている

RSA Factoring Challenge

2009年: RSA-768, 768bitの数が素因数分解された  
2000 CPU year

## RSA暗号：実際に鍵を作ってみよう

```
$ openssl genrsa 32 > private.txt
```

32ビットの鍵を作って, private.txt に保存する

```
$ cat private.txt
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
MC4CAQACBQDr1WRBAgMBAAECBQCs5O3BAgM
```

```
-----END RSA PRIVATE KEY-----
```

```
$ openssl rsa -text -in private.txt
```

```
Private-Key: (32 bit)
```

```
modulus: 3956630593 (0xebd56441)
```

$n=pq$

```
publicExponent: 65537 (0x10001)
```

$e$

```
privateExponent: 2900684225 (0xace4edc1)
```

$d$

```
prime1: 63299 (0xf743)
```

$p$

```
prime2: 62507 (0xf42b)
```

$q$