はじめに

廣瀬勝一

内容

- はじめに
- 整数論と代数の初歩
- 共通鍵暗号 (Symmetric Cryptosystem)
- 公開鍵暗号 (Asymmetric Cryptosystem)
- ディジタル署名 (Digital Signature Scheme)
- 暗号ハッシュ関数 (Cryptographic Hash Function)
- 個人識別 (Identification Scheme)
- 鍵共有 (Key exchange scheme)
- 秘密分散共有 (Secret Sharing Scheme)
- 擬似ランダム性 (Pseudorandomness)

講義資料と参考図書

`http://fuee.u-fukui.ac.jp/~hirose/lectures/`

情報通信工学特論のリンクをたどって下さい.

参考図書

- D. Stinson, Cryptography: Theory and Practice, CRC Press, 1995.
- D. Stinson, Cryptography: Theory and Practice, 2nd Ed., Chapman & Hall/CRC, 2002.
- D. Stinson, Cryptography: Theory and Practice, 3rd Ed., Chapman & Hall/CRC, 2006.
- A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

暗号とは何か？

不正な人為的操作から通信・記録の内容を守る技術

暗号の機能

秘匿	盗聴防止，プライバシ保護
認証・署名	改竄防止，本人確認，電子印鑑

暗号の歴史

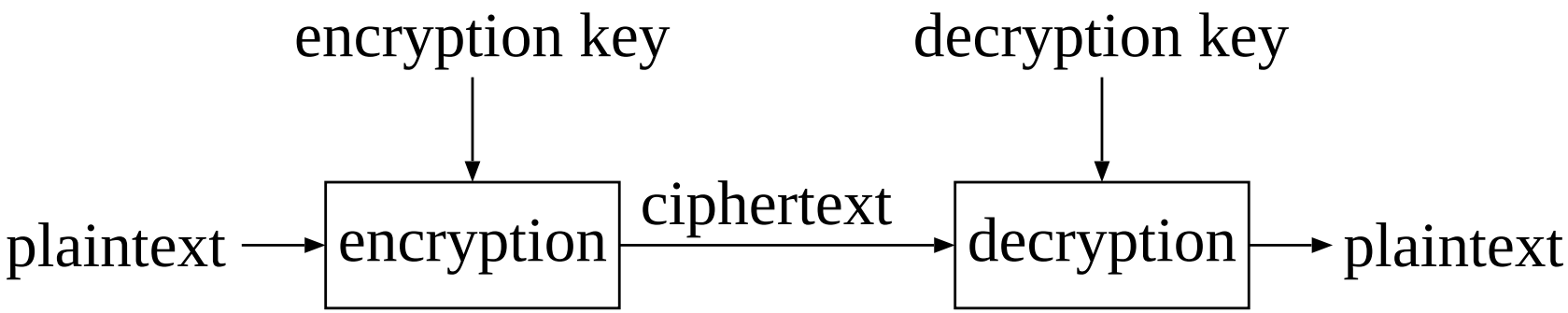
BC50 年頃	シーザ暗号 (換字暗号の一種)
	…
1939 年	第二次世界大戦
1975 年	DES (IBM)
1976 年	公開鍵暗号の考え (Diffie, Hellman)
1978 年	RSA (Rivest, Shamir, Adleman)
1984 年	ElGamal (ElGamal)
1986 年	Fiat-Shamir 法
1990 年	差分解読法 (Biham, Shamir)
1993 年	線形解読法 (松井)
2000 年	AES (Daemen, Rijmen)

暗号の急速な進歩の要因

計算機・ネットワークの発達と普及

- 電気通信
  盗聴，改竄が容易
- 日常の様々な活動・業務の電子化
  オンラインショッピング，電子商取引，電子現金
  - 社会的にも暗号が重要になってきた
  - 新しい暗号技術への要求
    公開鍵暗号，ディジタル署名，…
- 暗号解読の高速化，解読技術の発達

暗号系



- 平文 (plaintext)
- 暗号文 (ciphertext)

暗号化・復号アルゴリズムは公開されなければならない

シフト暗号

暗号化・復号鍵

a	b	c	d	e	f	g	h	i	j	k	l	m
X	Y	Z	A	B	C	D	E	F	G	H	I	J

n	o	p	q	r	s	t	u	v	w	x	y	z
K	L	M	N	O	P	Q	R	S	T	U	V	W

鍵の総数は 26

平文	t	h	i	s	i	s	n	o	t	s	e	c	r	e	t
暗号文	Q	E	F	P	F	P	K	L	Q	P	B	Z	O	B	Q

換字暗号 (Substitution Cipher)

暗号化・復号鍵

a	b	c	d	e	f	g	h	i	j	k	l	m
V	S	P	M	J	G	D	A	X	U	R	O	L

n	o	p	q	r	s	t	u	v	w	x	y	z
I	F	C	Z	W	T	Q	N	K	H	E	B	Y

鍵の総数は $26!(\approx 10^{26.6})$.

平文	t	h	i	s	i	s	n	o	t	s	e	c	r	e	t
暗号文	Q	A	X	T	X	T	I	F	Q	T	J	P	W	J	Q

転置暗号 (Permutation Cipher)

暗号化・復号鍵

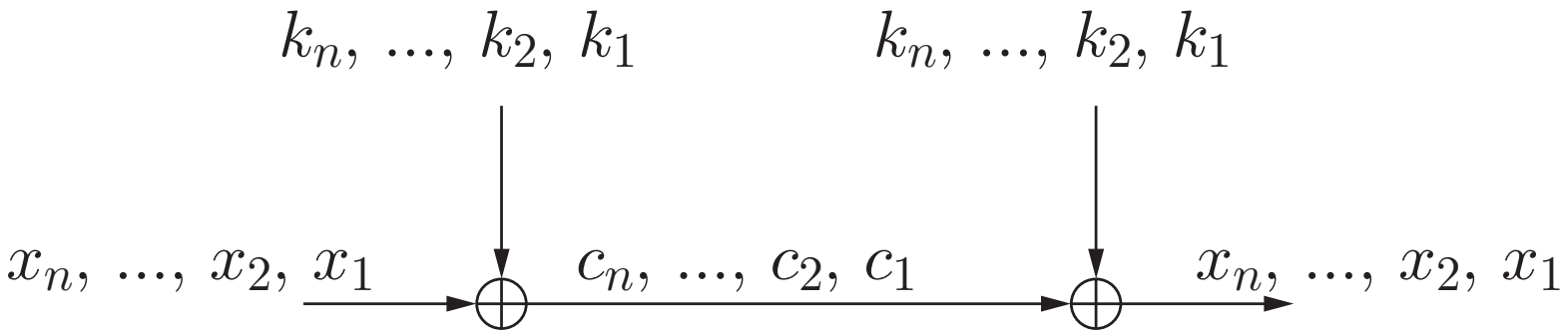
1	2	3	4	5
3	5	1	4	2

鍵の総数は 5!

平文	t	h	i	s	i	s	n	o	t	s	e	c	r	e	t
暗号文	I	I	T	S	H	O	S	S	T	N	R	T	E	E	C

ワンタイムパッド (One-Time Pad)

Vernam, 1917



$k_i, x_i, c_i \in \{0, 1\}$

$$c_i = x_i \oplus k_i$$

各 k_i が無作為に選択され，唯一度しか用いられなければ，この方式は情報理論的に安全である．