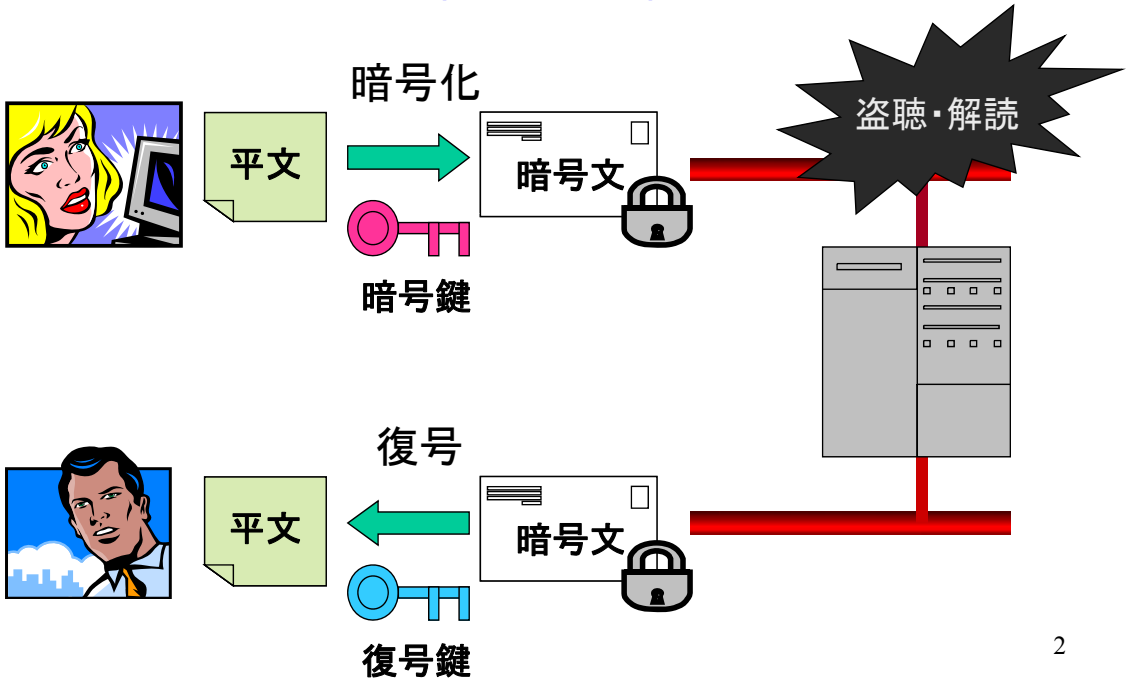
暗号技術　ー暗号とはー

- 暗号の歴史
- 簡単な暗号からより強い暗号へ
- 究極の暗号
- 暗号で署名する
- ネットワーク暗号

暗号技術　ーインターネット社会のセキュリティを護る技術ー

電子メールやクレジットカード情報を他人に知られないように
ネットワークで送りたい ⇒ 暗号による情報の秘匿（守秘機能）



暗号のお話（その1）

転置式暗号

・スキュタレー（木製の巻き軸）（スパルタ 紀元前5世紀）

・暗号化の例

平文：please come and visit me

PLEASE
QCOMEQ
ANDQVI
SITQME

暗号文：PQASLCNIEODTAMQQSEVMEQIE

暗号文：EIQEMVESQQMATDOEINCLSAQP

鍵：転置表と読み取り方

暗号のお話（その2） 換字式暗号（単アルファベット換字式暗号）

・シーザー暗号（カエサルシフト暗号）
（ローマ・共和政時代 ユリウス カエサル 紀元前1世紀）

平アルファベット：　a b c d e f g h i j l m n o p q r s t u v w x y z

暗号アルファベット：DEFGHIJKLMNOPQRSTUVWXYZABC

（ アルファベットを3文字ずらすこと ⇒ 鍵 ）（鍵の候補：25通り）

・鍵の作り方(例)

キーワード：MIYAZAKI AKIO ⇒ MIYAZKO

平アルファベット：　a b c d e f g h i j l m n o p q r s t u v w x y z

暗号アルファベット：MIYAZKOBCDEFGHJLNPQRSTUVWX

この換字式暗号は安全か？（暗号を解読することができるか？）

・鍵の候補 ⇒ アルファベット26文字の並べ替え（総数 $26! \cong 4 \times 10^{26}$ 通り）

1マイクロ秒 (10^{-6}秒) で1つの鍵を点検できるとして、
全ての鍵を点検し終えるのはいつ？ (1年 $\cong 3.2 \times 10^{7}$ 秒)

・言語のくせ（アルファベットの出現頻度）を利用する

文字（出現頻度%）

a (8.2)	b (1.5)	c (2.8)	d (4.3)	e (12.7)	f (2.2)	g (2.0)	h (6.1)
i (7.0)	j (0.2)	k (0.8)	l (4.0)	m (2.4)	n (6.7)	o (7.5)	p (1.9)
q (0.1)	r (6.0)	s (6.3)	t (9.1)	u (2.8)	v (1.0)	w (2.4)	x (0.2)
y (2.0)	z (0.1)						

⇒ 推理小説のネタ:
コナン・ドイル「踊る人形」（シャーロック・ホームズ物）、
エドガー・アラン・ポー「黄金虫」、江戸川乱歩「二銭銅貨」）

コナン・ドイル「踊る人形」

エドガー・アラン・ポー「黄金虫」

・・・・・ こう言って、ルグランは羊皮紙をまた熱して、私にそれを調べさせた。髑髏と山羊とのあいだに、赤い色で、次のような記号が乱雑に出ている。

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

「しかし」と私は紙片を彼に返しながら言った。「僕にゃあやっぱり、まるでわからないな。この謎（なぞ）を解いたらゴルコンダの宝石をみんなもらえるとしても、僕はとてもそれを手に入れることはできないねえ」・・・・・

暗号解読

- テキスト　英語
- 暗号方式　単アルファベット換字式暗号
- 暗号鍵　不明
  （⇒鍵の候補を総当り式にチェックするのは実用的ではない。）
- 暗号文の頻度分析
  暗号文に含まれるすべての記号（アルファベット）の出現頻度を調べる。
  （⇒論理的思考を必要とするが、それだけではなく、ズルをしたり（英語の辞書を使ったり）、直感に頼ったり、融通をきかせたり、当て推量をしたりする必要がある。）

言語のくせ（英語のアルファベットの出現頻度）

文字（出現頻度%）

a (8.2)	b (1.5)	c (2.8)	d (4.3)	e (12.7)
f (2.2)	g (2.0)	h (6.1)	i (7.0)	j (0.2)
k (0.8)	l (4.0)	m (2.4)	n (6.7)	o (7.5)
p (1.9)	q (0.1)	r (6.0)	s (6.3)	t (9.1)
u (2.8)	v (1.0)	w (2.4)	x (0.2)	y (2.0)
z (0.1)				

暗号文(その1)

PENW LSYBKNI OYSBSNF UYM KYI UEND EN MYBI PEN NYJPE FJZBPNI PEN MQD, ZQP EN UYM JBOEP;

PENW MYBI PEN UJBOEP ZJFPENJM UNJN LJYXW UEND PENW PJBNI PF CSW, ZQP PENW IBI;

PENW MYBI KW QDLSN UBSZQJ UYM KYI YM Y EYPPNJ YDI EN UYM.

暗号文(その1)

暗号解読(ステップ1)

P	E	N	W		L	S	Y	B	K	N	I		O	Y	S	B	S	N	F		U	Y	M		K	Y	I		U	E	N	D		E	N
t	h	e								e								e												h	e				h	e
M	Y	B	I		P	E	N		N	Y	J	P	E		F	J	Z	B	P	N	I		P	E	N		M	Q	D	,		Z	Q	P			
					t	h	e		e			t	h						t	e				t	h	e					,				t			
E	N		U	Y	M		J	B	O	E	P	;		P	E	N	W		M	Y	B	I		P	E	N		U	J	B	O	E	P			
h	e									h	t	;		t	h	e								t	h	e						h	t			
Z	J	F	P	E	N	J	M		U	N	J	N		L	J	Y	X	W		U	E	N	D		P	E	N	W		P	J	B	N	I		
			t	h	e					e		e									h	e			t	h	e			t			e			
P	F		C	S	W	,		Z	Q	P		P	E	N	W		I	B	I	;		P	E	N	W		M	Y	B	I		K	W			
t						,				t		t	h	e						;		t	h	e												
Q	D	L	S	N		U	B	S	Z	Q	J		U	Y	M		K	Y	I		Y	M		Y		E	Y	P	P	N	J		Y	D	I
				e																						h		t	t	e					
E	N		U	Y	M	.																															
h	e					.																														

暗号文の頻度分析

A	0				G	0				M	7				S	6				Y	10														
B	11				H	0				N	21	e	①		T	0				Z	5														
C	1				I	9				O	2				U	7																				
D	4				J	8				P	17	t	②		V	0																				
E	15	h	②		K	2				Q	4				W	8																				
F	3				L	2				R	0				X	1																				

暗号文(その1)

暗号解読(ステップ2)

P	E	N	W		L	S	Y	B	K	N	I		O	Y	S	B	S	N	F		U	Y	M		K	Y	I		U	E	N	D		E	N
t	h	e	y				a			e				a				e				a				a				h	e				h	e
M	Y	B	I		P	E	N		N	Y	J	P	E		F	J	Z	B	P	N	I		P	E	N		M	Q	D	,		Z	Q	P	
	a				t	h	e		e	a	r	t	h						t	e			t	h	e					,				t	
E	N		U	Y	M		J	B	O	E	P	;		P	E	N	W		M	Y	B	I		P	E	N		U	J	B	O	E	P			
h	e			a			r			h	t	;		t	h	e	y			a				t	h	e			r			h	t			
Z	J	F	P	E	N	J	M		U	N	J	N		L	J	Y	X	W		U	E	N	D		P	E	N	W		P	J	B	N	I		
	r		t	h	e	r				e	r	e			r	a		y			h	e			t	h	e	y		t	r		e			
P	F		C	S	W	,		Z	Q	P		P	E	N	W		I	B	I	;		P	E	N	W		M	Y	B	I		K	W			
t					y	,				t		t	h	e	y					;		t	h	e	y			a					y			
Q	D	L	S	N		U	B	S	Z	Q	J		U	Y	M		K	Y	I		Y	M		Y		E	Y	P	P	N	J		Y	D	I
				e							r			a				a			a			a		h	a	t	t	e	r		a		
E	N		U	Y	M	.																														
h	e			a		.																														

暗号文の頻度分析

A	0				G	0				M	7				S	6				Y	10	a	③													
B	11				H	0				N	21	e	①		T	0				Z	5															
C	1				I	9				O	2				U	7																					
D	4				J	8	r	③		P	17	t	②		V	0																					
E	15	h	②		K	2				Q	4				W	8	y	③																			
F	3				L	2				R	0				X	1																					

暗号文(その1)

暗号解読(ステップ3)

P	E	N	W		L	S	Y	B	K	N	I		O	Y	S	B	S	N	F		U	Y	M		K	Y	I		U	E	N	D		E	N
t	h	e	y				a			e	d			a				e			w	a	s			a			w	h	e			h	e
M	Y	B	I		P	E	N		N	Y	J	P	E		F	J	Z	B	P	N	I		P	E	N		M	Q	D	,		Z	Q	P	
s	a				t	h	e		e	a	r	t	h						t	e			t	h	e		s			,				t	
E	N		U	Y	M	s	J	B	O	E	P	;		P	E	N	W		M	Y	B	I		P	E	N		U	J	B	O	E	P			
h	e		w	a	s		r			h	t	;		t	h	e	y		s	a				t	h	e		w	r			h	t			
Z	J	F	P	E	N	J	M		U	N	J	N		L	J	Y	X	W		U	E	N	D		P	E	N	W		P	J	B	N	I		
	r		t	h	e	r	s		w	e	r	e			r	a		y		w	h	e			t	h	e	y		t	r		e			
P	F		C	S	W	,		Z	Q	P		P	E	N	W		I	B	I	;		P	E	N	W		M	Y	B	I		K	W			
t					y	,				t		t	h	e	y					;		t	h	e	y		s	a					y			
Q	D	L	S	N		U	B	S	Z	Q	J		U	Y	M		K	Y	I		Y	M		Y		E	Y	P	P	N	J		Y	D	I
				e		w					r		w	a	s			a			a	s		a		h	a	t	t	e	r		a		
E	N		U	Y	M	.																														
h	e		w	a	s	.																														

暗号文の頻度分析

A	0				G	0				M	7	s	④		S	6				Y	10	a	③													
B	11				H	0				N	21	e	①		T	0				Z	5															
C	1				I	9				O	2				U	7	w	④																			
D	4				J	8	r	③		P	17	t	②		V	0																					
E	15	h	②		K	2				Q	4				W	8	y	③																			
F	3				L	2				R	0				X	1																					

暗号文(その1)

暗号解読(ステップ4)

P	E	N	W		L	S	Y	B	K	N	I		O	Y	S	B	S	N	F		U	Y	M		K	Y	I		U	E	N	D		E	N
t	h	e	y				a	i		e	d			a		i		e			w	a	s			a	d		w	h	e	n		h	e
M	Y	B	I		P	E	N		N	Y	J	P	E		F	J	Z	B	P	N	I		P	E	N		M	Q	D	,		Z	Q	P			
s	a	i	d		t	h	e		e	a	r	t	h			r		i	t	e	d		t	h	e		s		n	,				t			
E	N		U	Y	M		J	B	O	E	P	;		P	E	N	W		M	Y	B	I		P	E	N		U	J	B	O	E	P			
h	e		w	a	s		r	i		h	t	;		t	h	e	y		s	a	i	d		t	h	e		w	r	i		h	t			
Z	J	F	P	E	N	J	M		U	N	J	N		L	J	Y	X	W		U	E	N	D		P	E	N	W		P	J	B	N	I		
	r		t	h	e	r	s		w	e	r	e			r	a		y		w	h	e	n		t	h	e	y		t	r	i	e	d		
P	F		C	S	W	,		Z	Q	P		P	E	N	W		I	B	I	;		P	E	N	W		M	Y	B	I		K	W			
t					y	,				t		t	h	e	y		d	i	d	;		t	h	e	y		s	a	i	d			y			
Q	D	L	S	N		U	B	S	Z	Q	J		U	Y	M		K	Y	I		Y	M		Y		E	Y	P	P	N	J		Y	D	I	
	n		l	e		w	i				r		w	a	s		m	a	d		a	s		a		h	a	t	t	e	r		a	n	d	
E	N		U	Y	M	.																															
h	e		w	a	s	.																															

暗号文の頻度分析

A	0				G	0				M	7	s	④		S	6				Y	10	a	③													
B	11	i	⑤		H	0				N	21	e	①		T	0				Z	5															
C	1				I	9	d	⑤		O	2				U	7	w	④																			
D	4	n	⑤		J	8	r	③		P	17	t	②		V	0																					
E	15	h	②		K	2				Q	4				W	8	y	③																			
F	3				L	2				R	0				X	1																					

暗号文(その1)

暗号解読(終了)

P	E	N	W		L	S	Y	B	K	N	I		O	Y	S	B	S	N	F		U	Y	M		K	Y	I		U	E	N	D		E	N
t	h	e	y		c	l	a	i	m	e	d		g	a	l	i	l	e	o		w	a	s		m	a	d		w	h	e	n		h	e
M	Y	B	I		P	E	N		N	Y	J	P	E		F	J	Z	B	P	N	I		P	E	N		M	Q	D	,		Z	Q	P			
s	a	i	d		t	h	e		e	a	r	t	h		o	r	b	i	t	e	d		t	h	e		s	u	n	,		b	u	t			
E	N		U	Y	M		J	B	O	E	P	;		P	E	N	W		M	Y	B	I		P	E	N		U	J	B	O	E	P			
h	e		w	a	s		r	i	g	h	t	;		t	h	e	y		s	a	i	d		t	h	e		w	r	i	g	h	t			
Z	J	F	P	E	N	J	M		U	N	J	N		L	J	Y	X	W		U	E	N	D		P	E	N	W		P	J	B	N	I		
b	r	o	t	h	e	r	s		w	e	r	e		c	r	a	z	y		w	h	e	n		t	h	e	y		t	r	i	e	d		
P	F		C	S	W	,		Z	Q	P		P	E	N	W		I	B	I	;		P	E	N	W		M	Y	B	I		K	W			
t	o		f	l	y	,		b	u	t		t	h	e	y		d	i	d	;		t	h	e	y		s	a	i	d		m	y			
Q	D	L	S	N		U	B	S	Z	Q	J		U	Y	M		K	Y	I		Y	M		Y		E	Y	P	P	N	J		Y	D	I	
u	n	c	l	e		w	i	l	b	u	r		w	a	s		m	a	d		a	s		a		h	a	t	t	e	r		a	n	d	
E	N		U	Y	M	.																															
h	e		w	a	s	.																															

暗号文の頻度分析

A	0				G	0				M	7	s	④		S	6	l	⑦		Y	10	a	③													
B	11	i	⑤		H	0				N	21	e	①		T	0				Z	5	b	⑥													
C	1	f	⑧		I	9	d	⑤		O	2	g	⑦		U	7	w	④																			
D	4	n	⑤		J	8	r	③		P	17	t	②		V	0																					
E	15	h	②		K	2	m	⑦		Q	4	u	⑥		W	8	y	③																			
F	3	o	⑥		L	2	c	⑧		R	0				X	1	z	⑧																			

暗号文（その１）の解読文（平文）

they claimed galileo was mad when he said the earth orbited the sun, but he was right;

they said the wright brothers were crazy when they tried to fly, but they did;

they said my uncle wilbur was mad as a hatter and he was.

暗号文（その２）

G XBLLXY EBNZYABLS BE G HGNCYAIJE LQBNC GNH G CAYGL HYGX IP BL BE GUEIXJLYXS PGLGX.

G WGN ZGNNIL UY LII ZGAYPJX BN LQY ZQIBZY IP QBE YNYWBYE.

暗号文（その2）

暗号解読（その2）

G	X	B	L	L	X	Y		E	B	N	Z	Y	A	B	L	S		B	E		G		H	G	N	C	Y	A	I	J	E
a		l	i	t	t	l	e		s	i	n	c	e	r	i	t	y		i	s		a		d	a	n	g	e	r	o	u	s

L	Q	B	N	C		G	N	H		G		C	A	Y	G	L		H	Y	G	X		I	P		B	L		B	E
t	h	i	n	g		a	n	d		a		g	r	e	a	t		d	e	a	l		o	f		i	t		i	s

G	U	E	I	X	J	L	Y	X	S		P	G	L	G	X	.
a	b	s	o	l	u	t	e	l	y		f	a	t	a	l	.

G		W	G	N		Z	G	N	N	I	L		U	Y		L	I	I		Z	G	A	Y	P	J	X		B	N		L	Q	Y
a		m	a	n		c	a	n	n	o	t		b	e		t	o	o		c	a	r	e	f	u	l		i	n		t	h	e

Z	Q	I	B	Z	Y		I	P		Q	B	E		Y	N	Y	W	B	Y	E	.
c	h	o	i	c	e		o	f		h	i	s		e	n	e	m	i	e	s	.

暗号文の頻度分析

A	4	r	
B	11	i	②
C	3	g	
D	0		
E	7	s	②
F	0		

G	14	a	①
H	3	d	③
I	8	o	④
J	3	u	
K	0		
L	11	t	③

M	0		
N	9	n	③
O	0		
P	4	f	⑤
Q	4	h	⑤
R	0		

S	2	y	
T	0		
U	2	b	
V	0		
W	2	m	⑤
X	7	l	④

Y	13	e	⑤
Z	5	c	④

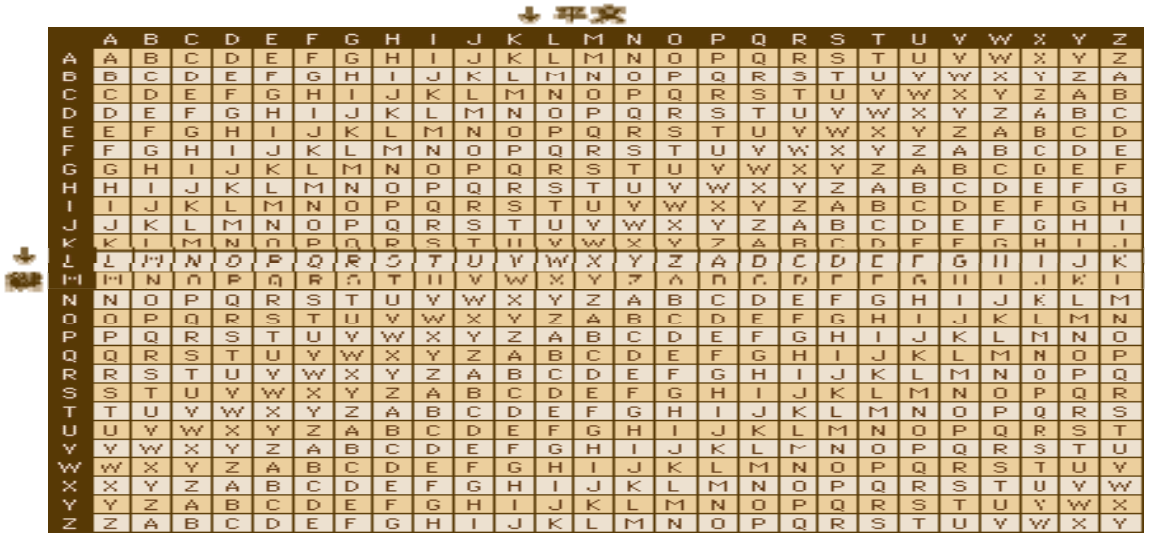
暗号文（その2）の解読文（平文）

a little sincerity is a dangerous thing and a great deal of it is absolutely fatal.

a man cannot be too careful in the choice of his enemies.

ヴィジュネル暗号（多表換字式暗号）

ヴィジュネル方陣（26種類の暗号アルファベット）



暗号化の方法

●キーワードを選ぶ（例: KING）。

●平文アルファベットを1文字づつ10番目(K)、8番目(I)、13番目(N)、6番目(G)の暗号アルファベットを用いて暗号化する。

ヴィジュネル暗号（多表換字式暗号）

・暗号化の例

平文: t h e r e i s a n e g g o n t h e t a b l e ・・・

キーワード: K I N G K I N G K I N G K I N G K I ・・・

暗号文: D P R X O Q F G X M T M Y V G N O B N H V M ・・・

鍵（キーワード：できればランダムに選ぶ）の長さをある程度長くすれば鍵の全数探索に対しては安全となる。
しかし、鍵の長さをいろいろ仮定して暗号文の頻度分析を行うことにより、解読される可能性もある！

エニグマ暗号機（ドイツ・第二次世界大戦中に使用）

- 暗号機の基本原理は、鍵（キーワード）の長さが 26×26×26＝17,576 のヴィジュネル暗号（←3個のローター（回転盤・26個の歯車）の回転周期）
- ローターの初期値と順序、プラグボードの配線を変えることができ、鍵の総数は 約1京＝約1,000兆×10

ネットワーク暗号（大規模ネットワークのための暗号）（1）

- 非常に多くの人が使う、通信相手はさまざま、未知の人との通信、・・・

⇒ 鍵配送方式：「メッセージを送る側と受ける側でどのように鍵を配送するか？」（ネットワーク暗号を実現するための「鍵」）

- 暗号のしくみも共通のものを用いるほうが便利

⇒ 暗号のしくみが知られても暗号の安全性が保てるならば、暗号の仕組みを公開し、標準化する。

- “フェイス・トゥ・フェイス”でないので、メッセージ（文書）が偽造や改ざんされたものでなく、正当な相手から送られてきたものであることを確認できる機能も必要

⇒ 暗号による認証機能（メッセージ認証機能、文書認証機能）

ネットワーク暗号（大規模ネットワークのための暗号）（2）

安全で便利なネットワークを実現するには、

◆ そのしくみを公開しても安全な暗号方式

情報量的に安全な暗号：
「ランダムに選ぶ鍵の長さ」＝「平文の長さ」

計算量的に安全な暗号：平文を推定するのに、スーパーコンピュータを何台も使っても天文学的時間がかかる。

◆ 鍵配送方式

◆ 署名や捺印の機能を実現する認証機能