情報科学序説 (第6回)

IT社会における情報セキュリティ

情報セキュリティって何？

情報システム・ネットワークの安全性

セキュリティを守るための技術 (特に、暗号技術)

平成24年5月23日 (水)

情報科学部

宮崎明雄

情報科学序説（第6回）
IT社会における情報セキュリティ

レポート課題

〔課題1〕、〔課題2〕のいずれか一つを選択し、レポートにまとめなさい。なお、レポートの分量はA4用紙1枚とする（ただし、用紙の両面を使用して構わない）。

（注意）第1回目のレポートについて：
① 第4回～第6回の講義に対して、レポートを一つ提出しなければならない。ただし、欠席した講義に関するレポートは不可。
② 提出期限は、第6回の講義日から一週間後（つまり、第7回の講義日）の17時まで（提出先：情報科学部事務室レポート箱）

（注意）レポートには必ず下記の事項を明記すること。
情報科学序説レポート（第○回）、担当：○○○○先生、
学年、学籍番号、氏名

〔課題1〕

情報セキュリティに関する今日の講義の内容についてまとめ、自分の感想・意見を述べなさい。

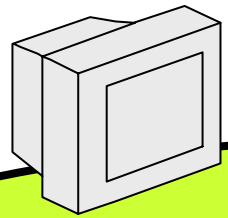
〔課題2〕

「情報セキュリティに関して、自分の身近なところでどのような問題が起きているか？」について調べ、このような問題が起きる背景、このような問題に対する対応策など、自分の感想・意見を述べなさい。

インターネット社会における情報セキュリティ

マスメディア情報：
テレビ放送、
ラジオ放送、
ビデオ映画、
電子新聞、
オンライン雑誌、
電子書籍、
・・・・・・

公的情報・私的情報：電話、FAX、電子メール、・・・・



インターネット
(高速ネットワーク)

双方向通信・双方向機能

IT革命の中核は放送と通信が融合するメディア・ビッグバンである

テレビとパソコンが有機的に合体
●インターネットの中にテレビ映像が流れる
●テレビがインターネット端末になる
～ホームページ検索、eショッピング、電子メール送受信～

マイクロプロセッサ、システムＬＳＩ、インターネット、
光通信・衛星通信・無線通信技術、ディジタル技術

インターネット社会の問題点

- 匿名性：IDとパスワードで個人を認証・識別
  ⇒ なりすまし
- 不特定多数性：電子掲示板、電子メール
  ⇒ 未知の人との容易なコンタクト
- 時間的・地理的な無制限性：広域コミュニケーション
  ⇒ 国境のない世界
- 情報発信場所の不特定性、電子データの無痕跡性（容易に完全抹消）
  ⇒ 犯罪の痕跡が残りにくい
- 電子商取引の増大：インターネットを利用した金銭の取り扱い
  ⇒ 契約書などの文書の偽造・改ざん、取り引き内容・取り引き事実の事後否認
- インターネットを利用した音楽、画像、映像の配信：デジタル放送、ネット放送、コンテンツ配信サービス
  ⇒ コンテンツの不正コピー、コンテンツの無断編集・無断使用
- インターネットと企業情報ネットワークの結合
  ⇒ 通信路上でのデータの傍受、ファイルの不当な読み出し、ファイルの改ざん・破壊

インターネット

盗聴

なりすまし

改ざん

ウイルス

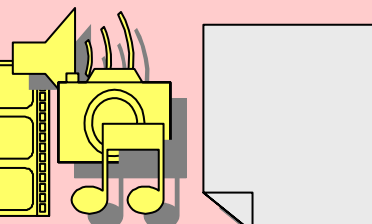
パスワード漏洩

データ漏洩
不正持ち出し

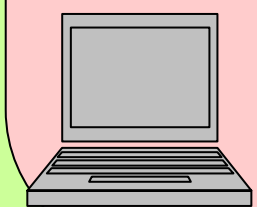
ウイルス感染

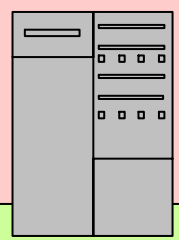
データ改ざん

不正コピーによる
持ち出し



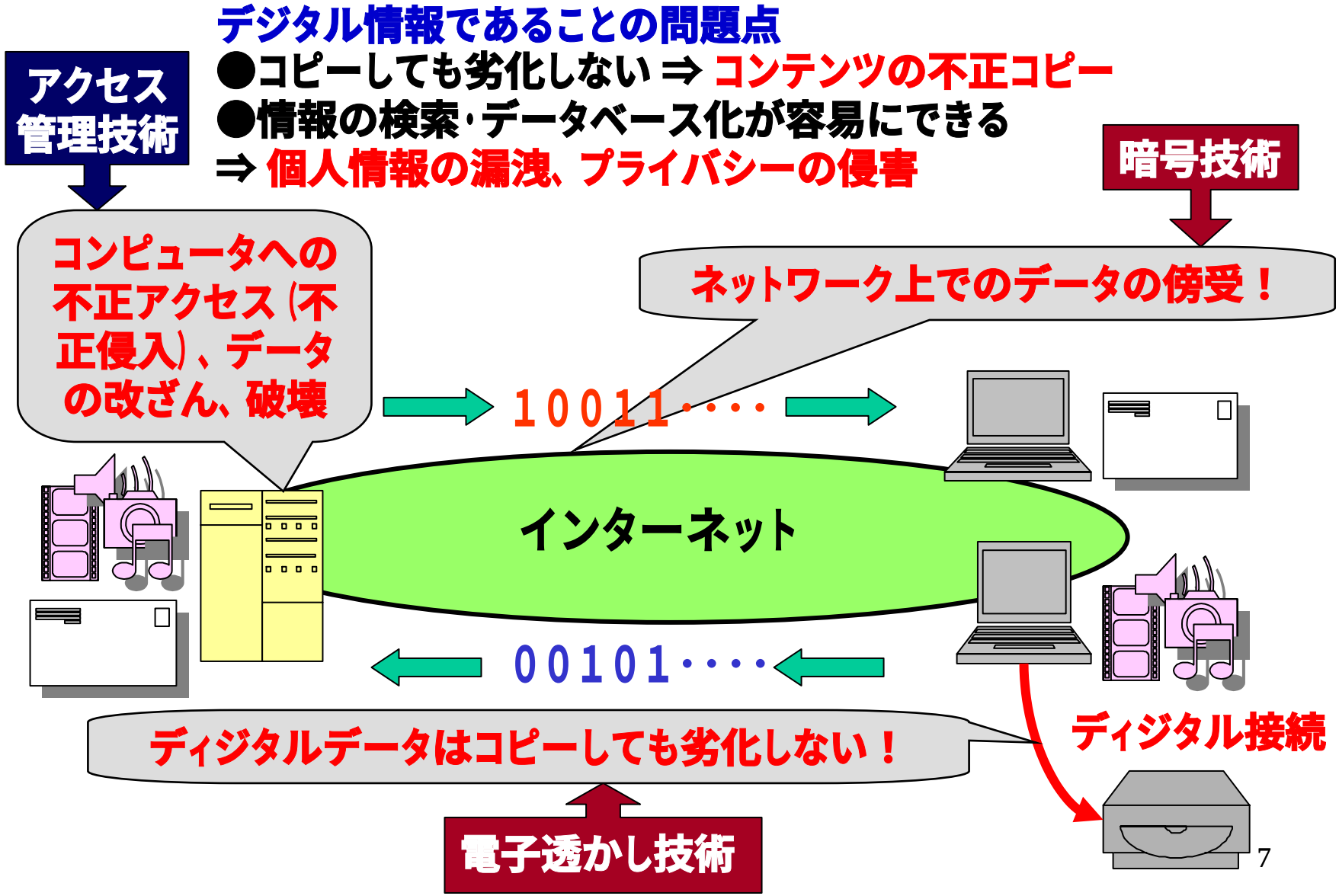
文書、音声、オーディオ、
画像・映像、・・・



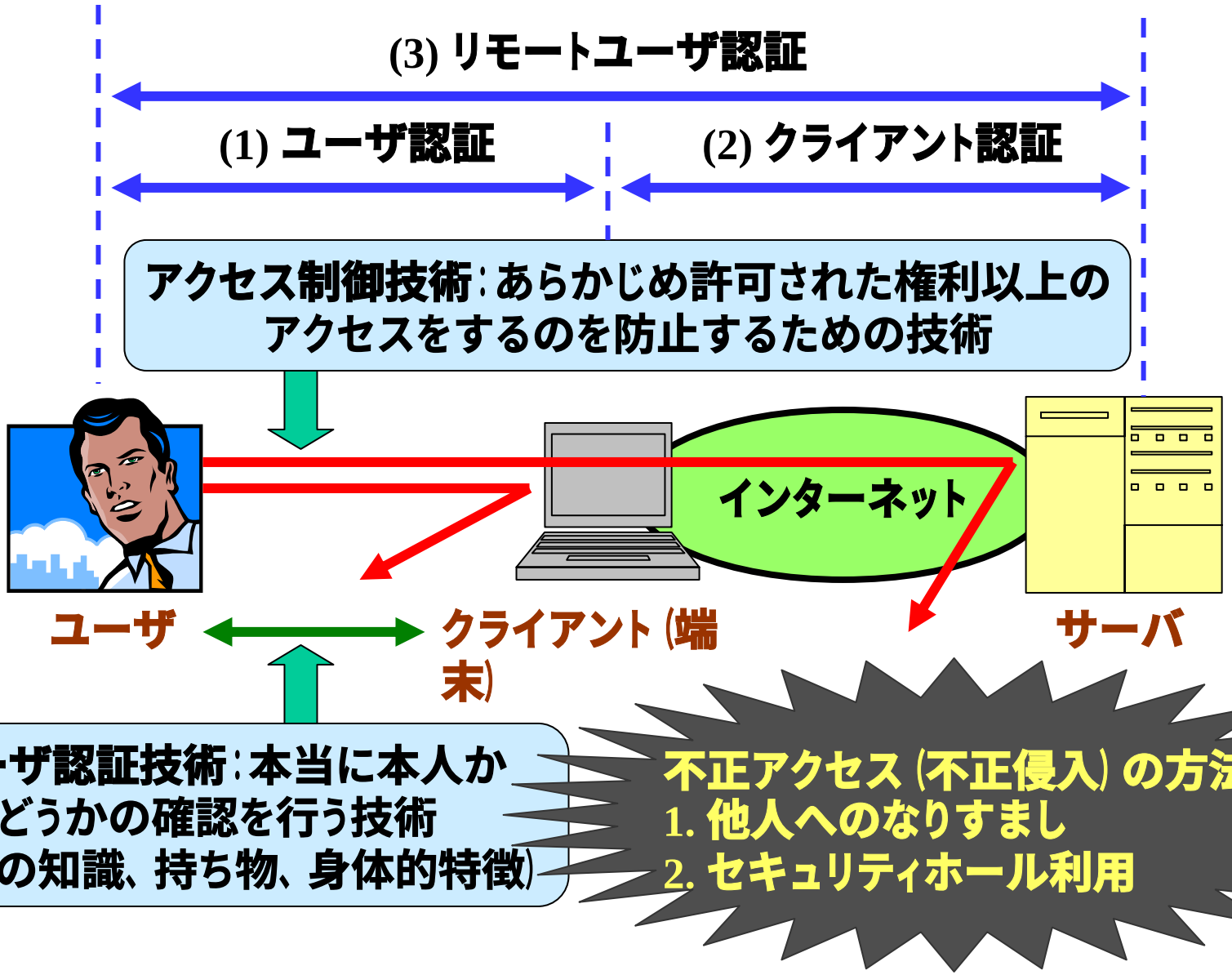


イントラネット（会社・学校）

インターネット社会におけるデジタル情報の保護



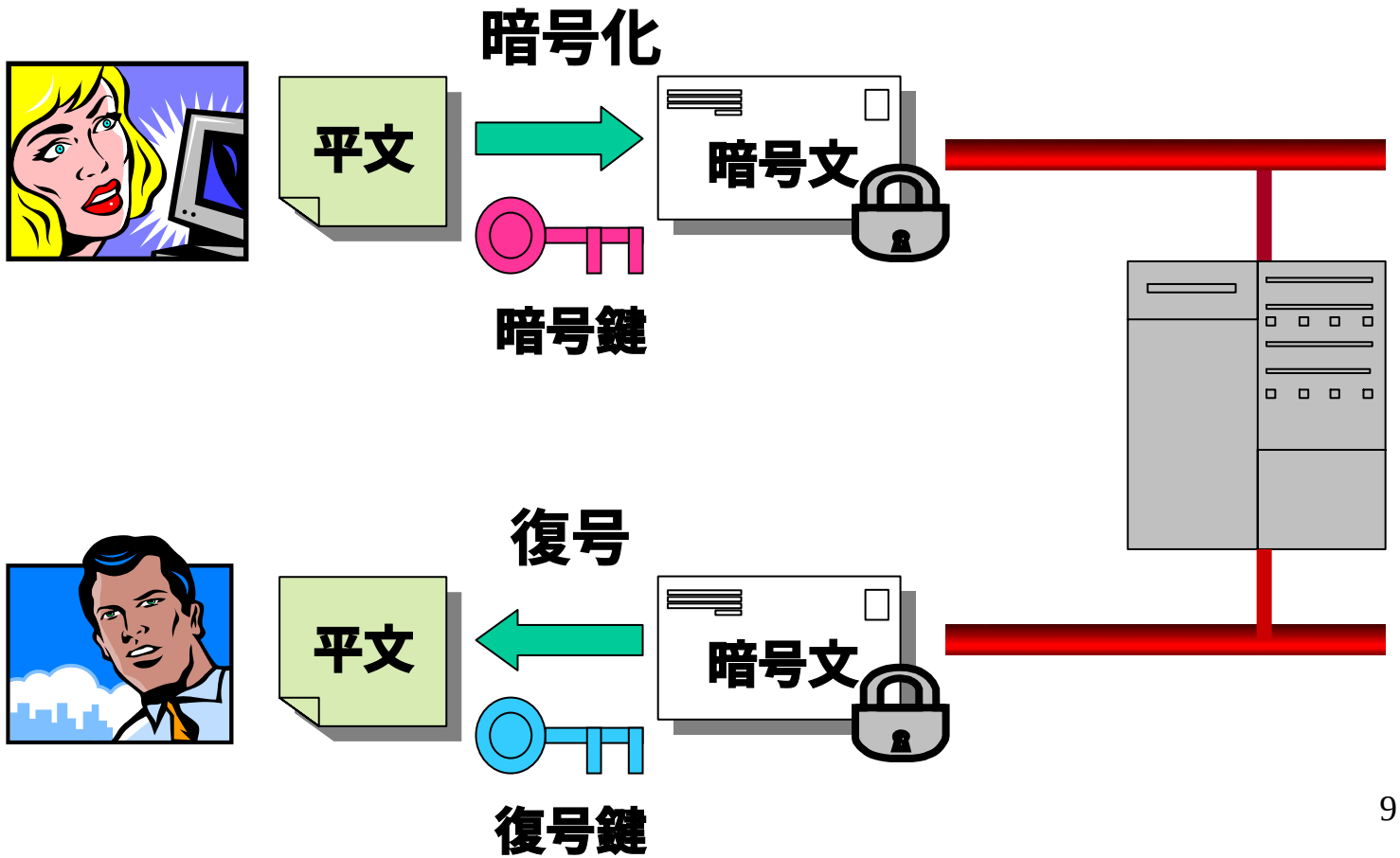
アクセス管理技術　ーインターネット社会のセキュリティを護る技術ー



暗号・認証技術　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**

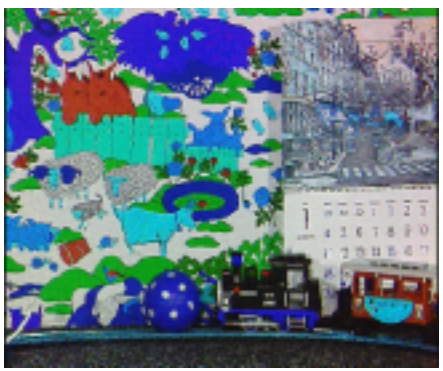
送り手や通信内容の認証 ⇒ **暗号による情報の認証（電子署名）**



電子透かし（Digital Watermark）技術
－インターネット社会のセキュリティを護る技術－

著作権やコピー制御などの情報をディジタルコンテンツの中に、本来のコンテンツ品質を損なわず、人間に知覚されないように埋め込む（忍び込ませる）技術

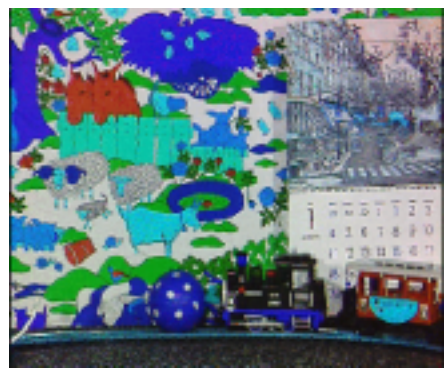
主情報　　副情報



＋

著作権情報
会社ロゴマーク
購入者情報

→

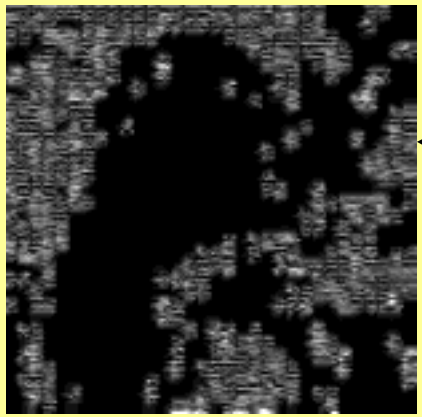


原画像　　透かし情報　　透かし入り画像

【電子透かしの埋め込み例】

原画像

透かし入り画像

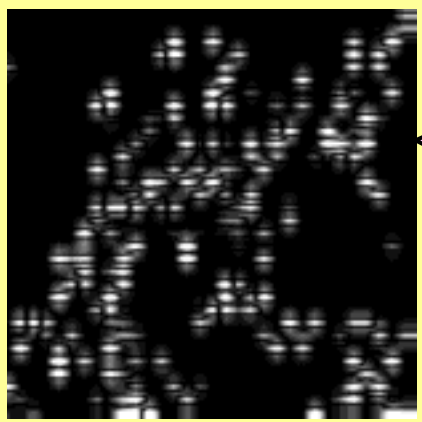


差分画像（32倍強調）

画像の平坦な部分や単調な部分に405ビットの透かし情報が埋め込まれている！

原画像

透かし入り画像

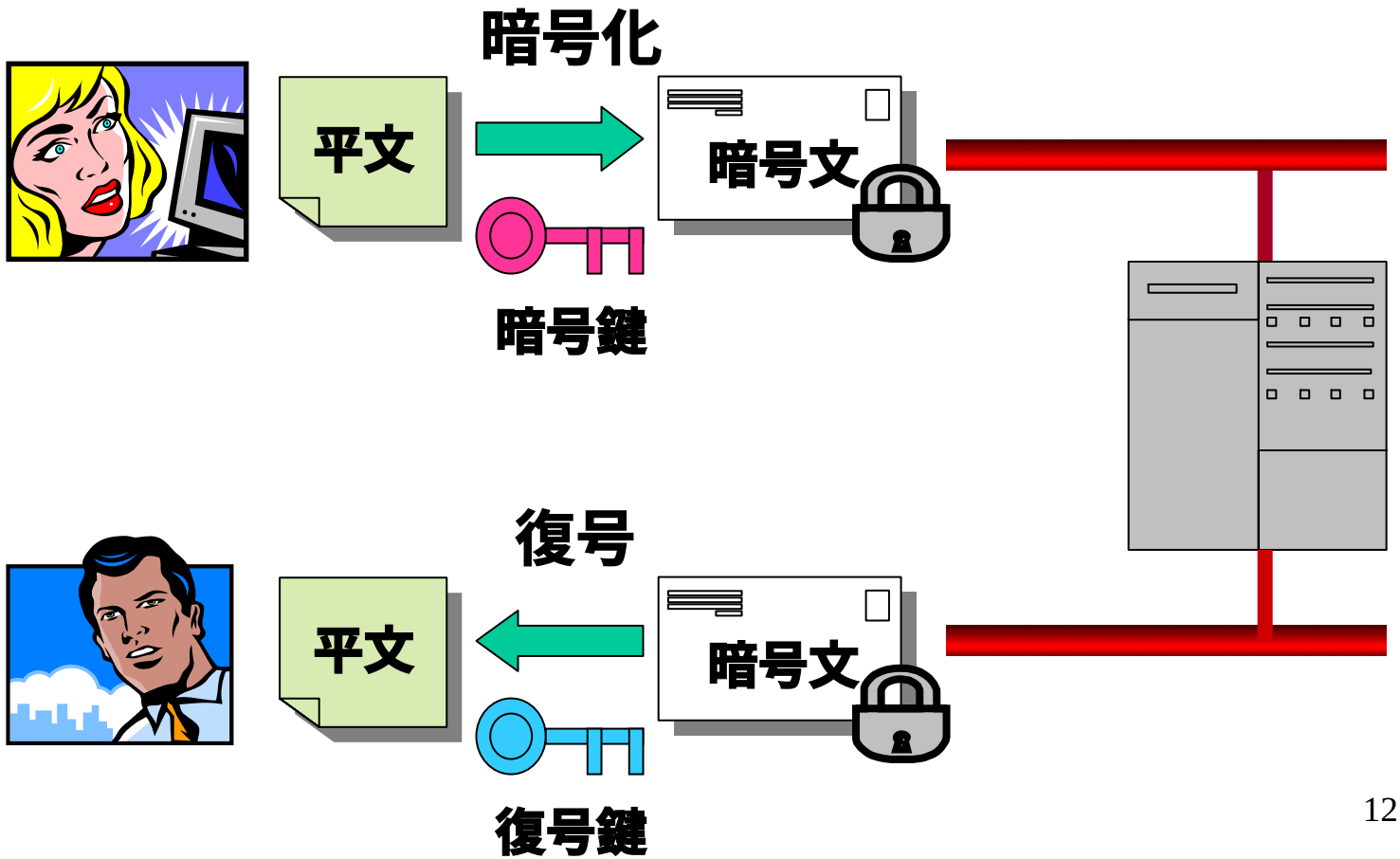


差分画像（32倍強調）

画像の輪郭線や複雑な部分に209ビットの透かし情報が埋め込まれている

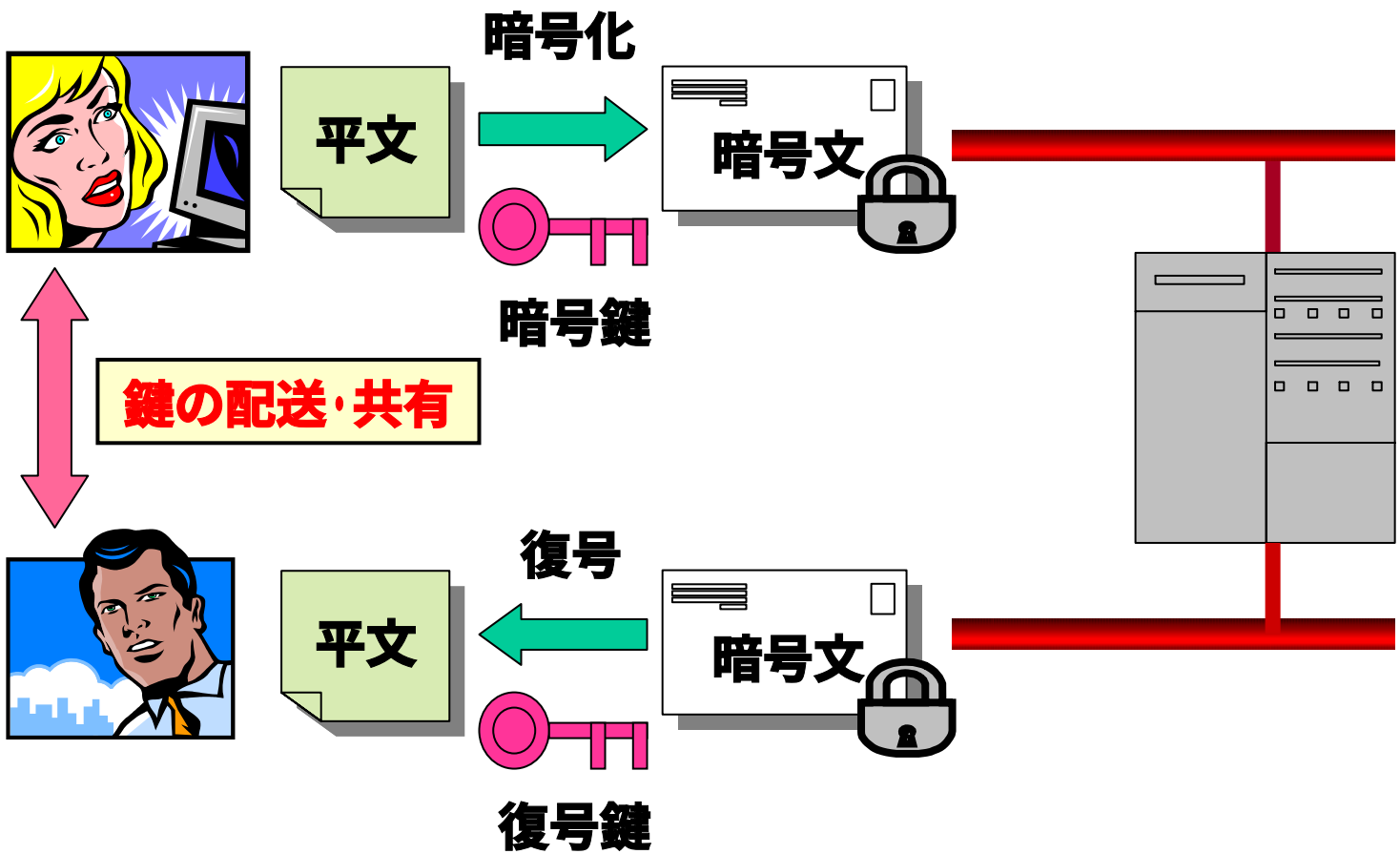
暗号技術　ー暗号のしくみー

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**



共通鍵暗号／秘密鍵暗号

- 暗号鍵＝復号鍵　⇒　**鍵の配送問題**
- 転置式暗号、換字式暗号、・・・・
- DES (Data Encryption Standard) **暗号**



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

・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ナノ秒 (10^{-9}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%）

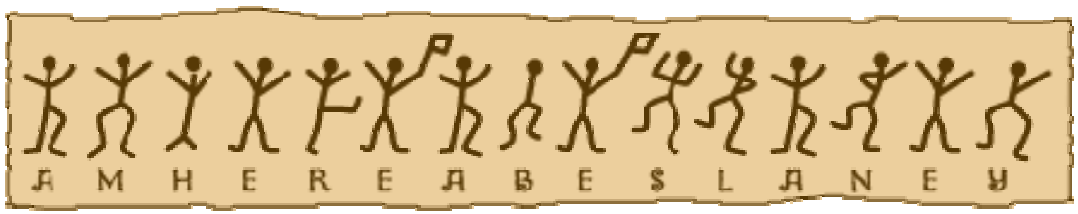
a (8.2)	b (1.5)	c (2.8)	d (4.3)	e (12.7)	f (2.2)	g (2.0)	h (6.1)
i (7.0)	j (0.2)	k (0.8)	l (4.0)	m (2.4)	n (6.7)	o (7.5)	p (1.9)
q (0.1)	r (6.0)	s (6.3)	t (9.1)	u (2.8)	v (1.0)	w (2.4)	x (0.2)
y (2.0)	z (0.1)						

⇒ 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」

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

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		
B	11		
C	1		
D	4		
E	15	h	②
F	3		

G	0		
H	0		
I	9		
J	8	r	③
K	2		
L	2		

M	7		
N	21	e	①
O	2		
P	17	t	②
Q	4		
R	0		

S	6		
T	0		
U	7		
V	0		
W	8	y	③
X	1		

Y	10	a	③
Z	5		

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		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		
B	11	i	⑤
C	1		
D	4	n	⑤
E	15	h	②
F	3		

G	0		
H	0		
I	9	d	⑤
J	8	r	③
K	2		
L	2		

M	7	s	④
N	21	e	①
O	2		
P	17	t	②
Q	4		
R	0		

S	6		
T	0		
U	7	w	④
V	0		
W	8	y	③
X	1		

Y	10	a	③
Z	5		

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		
B	11	i	⑤
C	1	f	⑧
D	4	n	⑤
E	15	h	②
F	3	o	⑥

G	0		
H	0		
I	9	d	⑤
J	8	r	③
K	2	m	⑦
L	2	c	⑧

M	7	s	④
N	21	e	①
O	2	g	⑦
P	17	t	②
Q	4	u	⑥
R	0		

S	6	l	⑦
T	0		
U	7	w	④
V	0		
W	8	y	③
X	1	z	⑧

Y	10	a	③
Z	5	b	⑥

暗号文の解読文 (＝平文)

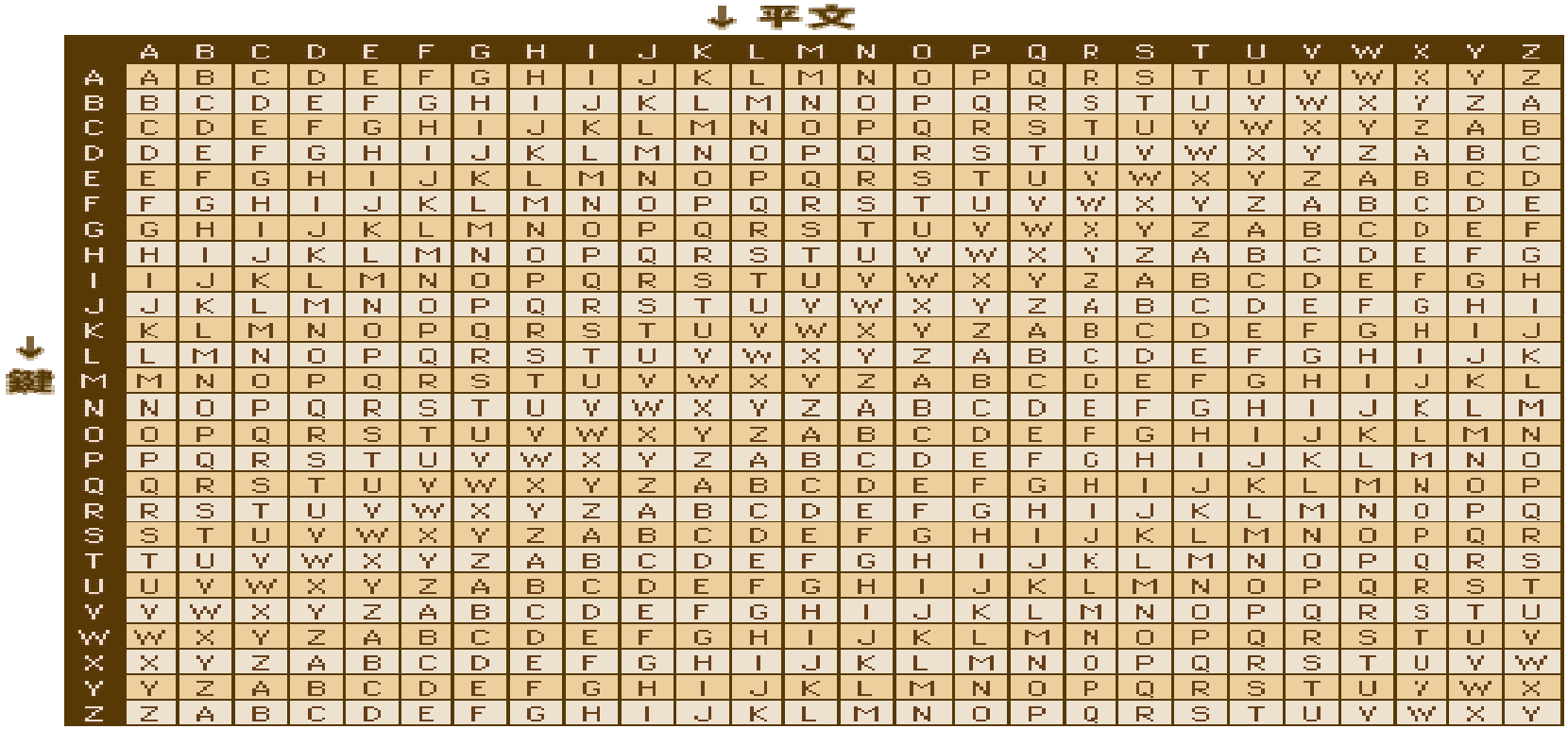
they claimed galileo was mad when he said the earth orbited the sun, but he was right;

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.

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)



鍵＼平文	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

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 NGK IN G K I NG K I NGK I NG KI ・・・

暗号文：　D PRXO QF GX MTM YV GNO BNHVM ・・・

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（回転盤・26個の歯車）の回転周期）
- ロータの初期値と順序、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＝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）

- 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。

- 暗号のメッセージ認証機能、文書認証機能

⇒ メッセージ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

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

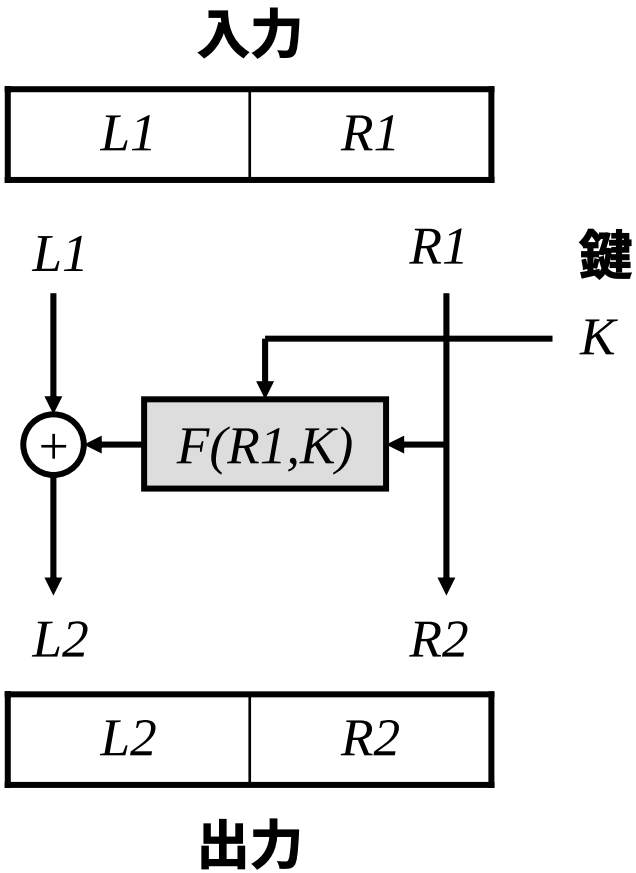
◆ 鍵配送方式

◆ 署名や捺印の機能を実現するメッセージ認証機能

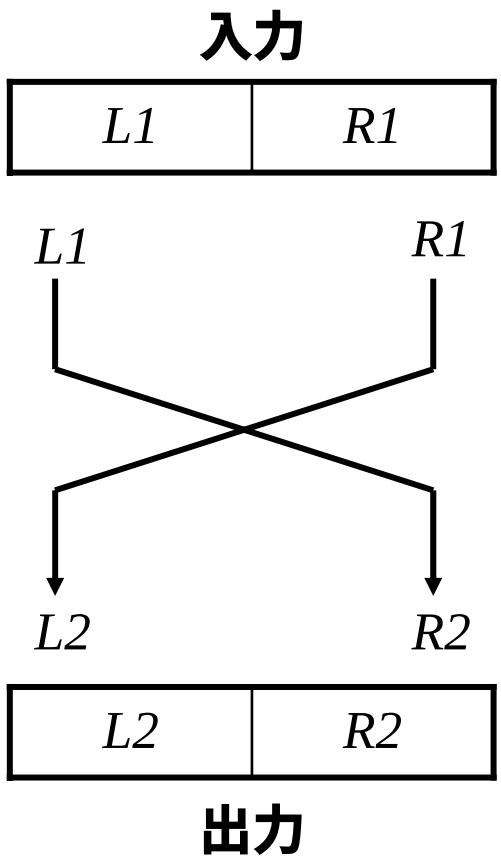
DES (Data Encryption Standard, データ暗号化規格)

- 1974年：IBMにより開発される。
- 1977年：アメリカ連邦政府の標準暗号となる。
- ブロック暗号 (*n* ビットブロック暗号)
  平文 64 or 124 ビット ⇒ 暗号文 64 or 128 ビット
- 鍵の長さ (鍵長) 56 ビット
- 暗号のしくみを完全に公開 ⇒ 従来の暗号のイメージを完全に変える。「暗い」暗号から「明るい」暗号へ。ネットワーク暗号、現代暗号の幕開け。
- フェイステル型暗号 ⇒ 基本変換AとBを繰り返す構造をもつ。
- 繰り返し型ブロック暗号

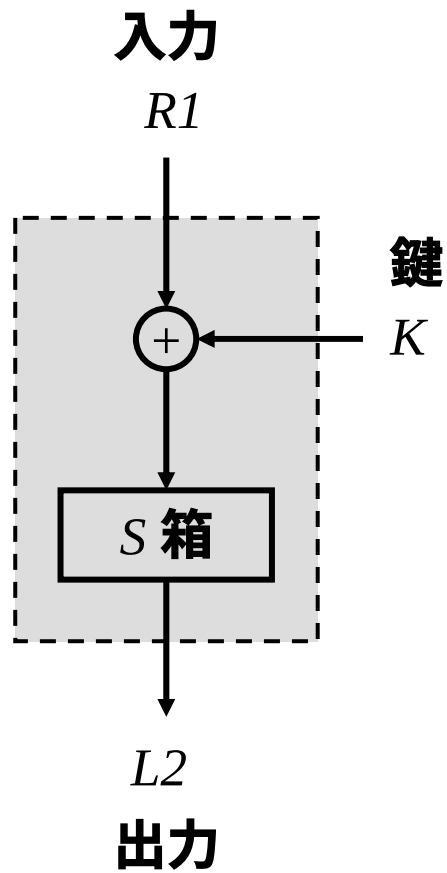
DES (Data Encryption Standard) 暗号 (1)



基本変換A

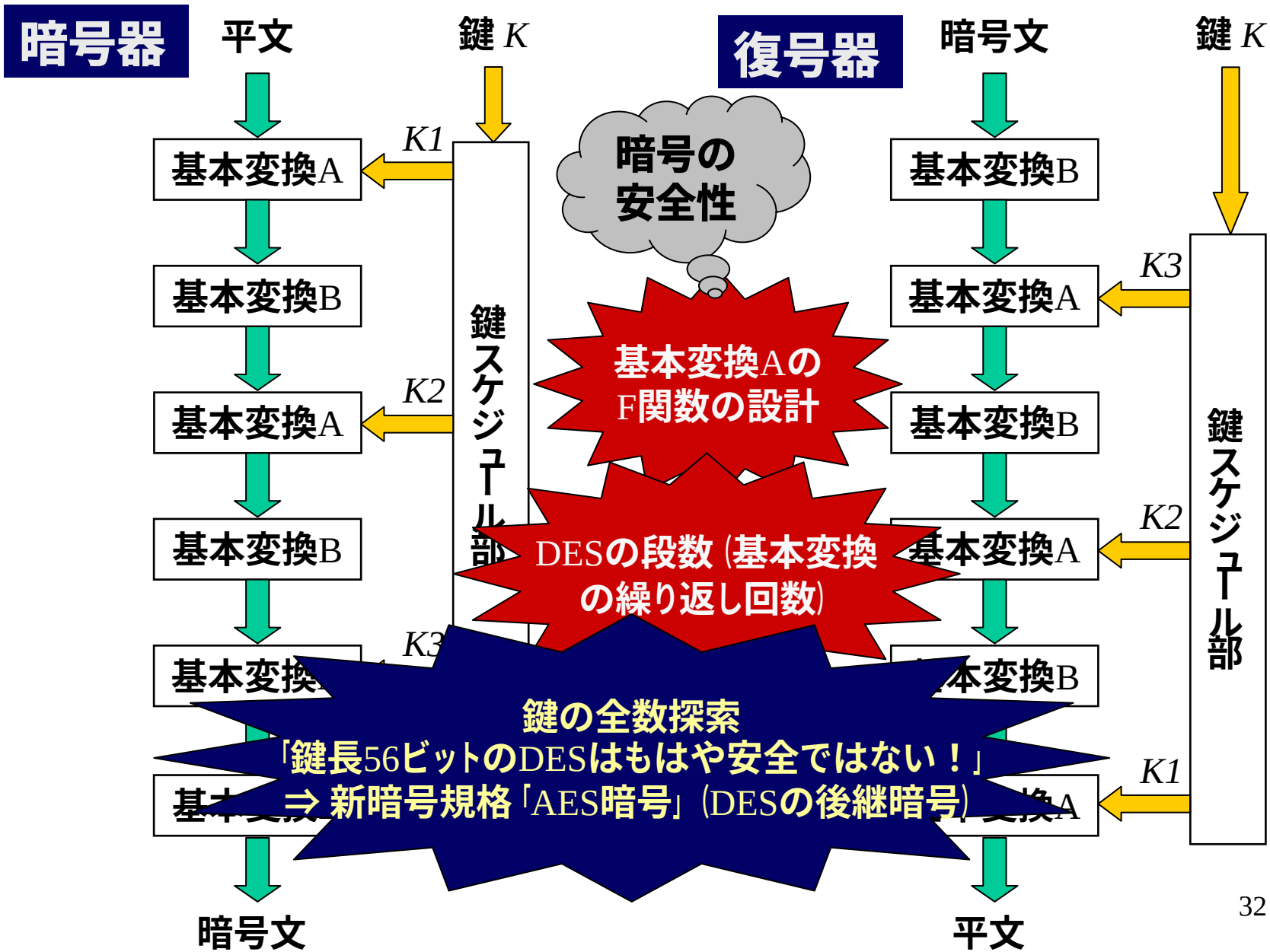


基本変換B



基本変換Aの
*F*関数の例

DES (Data Encryption Standard) 暗号（2）



公開鍵暗号／複数鍵暗号

- **秘密鍵と公開鍵**（暗号鍵≠復号鍵）
  - －秘密鍵で暗号化、公開鍵で復号
  - －公開鍵で暗号化、秘密鍵で復号
  - －公開鍵から秘密鍵を推定するのは現状では困難
    （整数論、楕円関数論など数学の理論で保証）
- **鍵の配送が不要**
- **情報の秘匿**だけでなく、**情報の認証**にも使える
- 電子署名（電子印鑑）、電子投票、電子マネー、電子商取引（Eーコマース）での利用
- RSA（Rivest, Shamir, Adelman）暗号、楕円曲線暗号

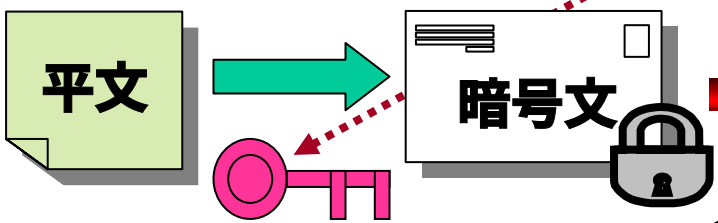
公開鍵暗号による情報の秘匿

アリスからボブへ暗号化してメールを送る

公開鍵一覧表

暗号化

アリス

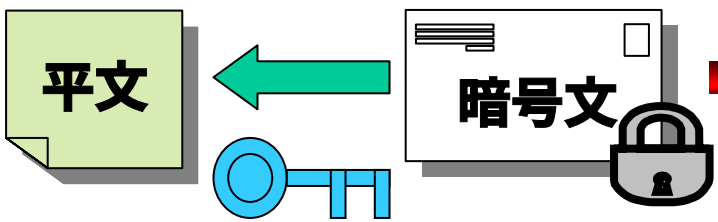


ボブの公開鍵

公開鍵暗号方式と
身近な類似の例
⇒ マンション（集合
住宅）の郵便受け

復号

ボブ



ボブの秘密鍵

RSA暗号（R.L.Rivest, A.Shamir, L.Adleman)

Bob の公開鍵･秘密鍵の生成

① Bob は二つの素数 p, q をランダムに選び、その積 n = pq を計算する。

② k = LCM(p-1,q-1)（LCM：最小公倍数）を計算し、k と最大公約数が 1 となる正整数 e を一つ選び、 e と n の組 (e,n) を公開鍵ファイルに Alice の公開鍵として登録する。

③ [ed] mod k = 1 となる d を計算し、これを秘密鍵として秘密に保管する。

RSA暗号（R.L.Rivest, A.Shamir, L.Adleman）

Alice から Bob への暗号通信

① Alice は公開鍵ファイルから Bob の公開鍵 (e,n) を調べる。

② Alice は平文 M を 0 以上 n-1 以下の整数で表し、それを e乗し、n で割った余り C = [M^e] mod n を計算し、C を暗号として送る。

③ Bob は受け取った暗号文 C を d乗し、n で割った余り [C^d] mod n を計算して復号を行う。

RSA暗号の安全性： 秘密鍵を求めるには、k すなわち p, q が分からないといけない。しかし、p, q が非常に大きな素数の場合、n = pq を素因数分解するのは大変難しい！（一方向性関数）

RSA暗号の例

公開鍵･秘密鍵の生成

① p=5, q=11 とすると n=pq=55 となる。

② k = LCM(p-1,q-1) = LCM(4,10) = 20となる。k と最大公約数が 1 となる正整数として e=3 を選ぶ。(e,n)=(3,55) を公開鍵とする。

③ [ed] mod k = [3d] mod 20 = 1 より d=7 を秘密鍵とする。

暗号通信

① **暗号化：** 平文を M=4 とすると 暗号文は C = [M^e] mod n = [4^3] mod 55 = 9 となる。

② **復号化：** 暗号文を C=9 とすると、[C^d] mod n = [9^7] mod 55 = 4 となり、平文 M=4 が得られる。

【素因数分解問題】 次の数を素因数分解せよ

(a) 504233 (b) 2077003 (c) 71255441

(a) 587×859
(b) 683×3041
(c) 9749×7309

公開鍵暗号による情報の秘匿と認証

アリスからボブへ暗号化してメールを送る
ボブはアリスからのメールであることを認証できる

アリス

暗号化

平文

暗号文

アリスの秘密鍵

公開鍵一覧表

ボブ

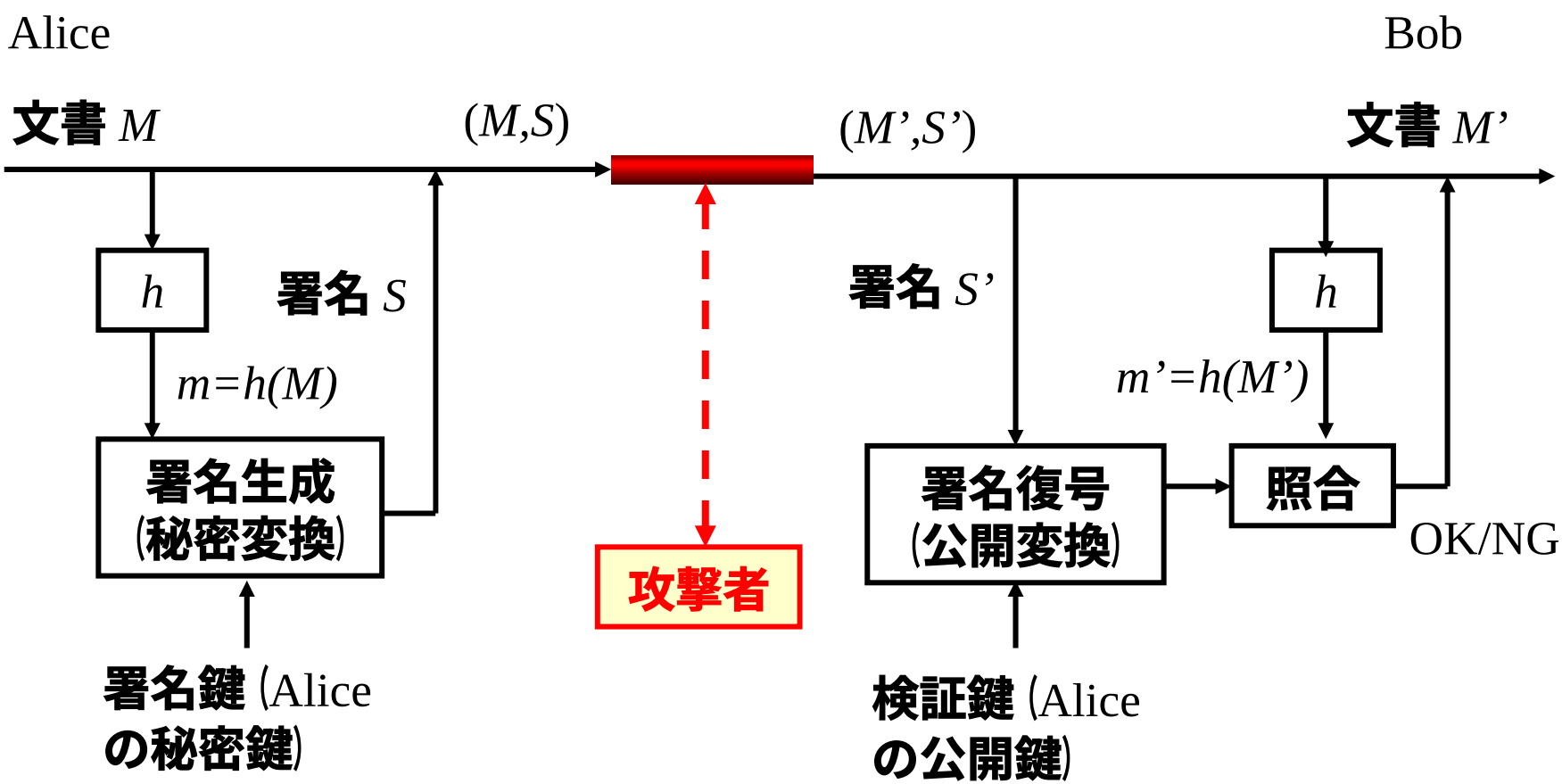
復号

平文

暗号文

アリスの公開鍵

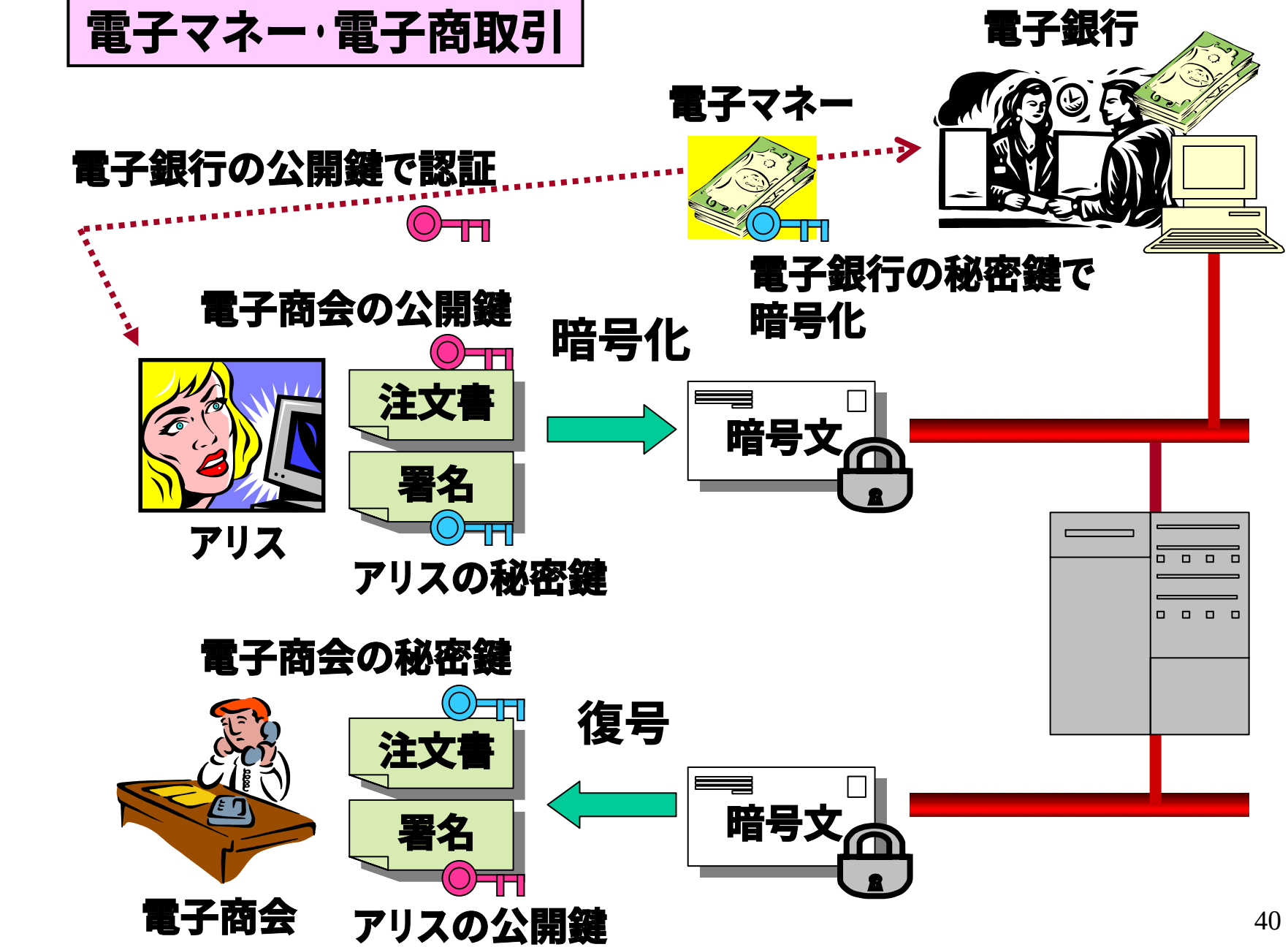
電子署名（ディジタル署名）　－認証のしくみ－



h：**ハッシュ関数（衝突困難ハッシュ関数）**

SHA-1 (Secure Hash Algorithm 1), MD5 (Message Digest 5), ・・・

電子マネー・電子商取引


電子銀行
電子マネー
電子銀行の公開鍵で認証
電子銀行の秘密鍵で
暗号化
電子商会の公開鍵
暗号化
注文書
署名
暗号文
アリス
アリスの秘密鍵
電子商会の秘密鍵
復号
注文書
署名
暗号文
電子商会
アリスの公開鍵

参考文献

- 佐々木良一、他、インターネット時代の情報セキュリティ　暗号と電子透かし、共立出版、2000年.
- 豊田 豊、わかりやすい暗号学 ーセキュリティを護るためにー、米田出版、2000年.
- 今井秀樹、明るい暗号の話 ーネットワーク社会のセキュリティ技術ー、裳華房、1998年.
- 辻井重男、暗号と情報社会、文春新書、1999年.
- 辻井重男、暗号 ーポストモダンの情報セキュリティーー、講談社選書、1996年.
- 太田和夫、黒澤馨、渡辺治、情報セキュリティの科学 ーマジックプロトコルへの招待ー、講談社ブルーバックス、1995年.
- 西垣 通、IT革命 ーネット社会のゆくえー、岩波新書、2001年.
- ルドルフ・キッペンハーン (赤根洋子訳) 、暗号攻防史、文春文庫、2001年.
- サイモン・シン (青木薫訳) 、暗号解読 ーロゼッタストーンから量子暗号までー、新潮社、2001年.