

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23年5月23日(月)

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。

(注意) 第1回目のレポートについて:

第3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。

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〕

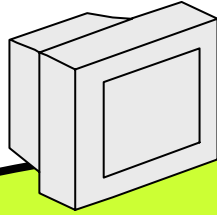
情報セキュリティに関する今日の講義の内容についてまとめ、自分の感想・意見を述べなさい。

〔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

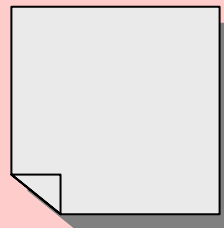
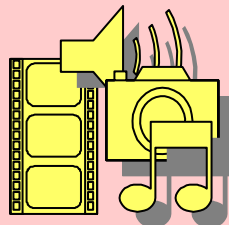
なりすまし

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)



- **情報セキュリティとは何か？ IT社会・ネットワーク社会において、私たちが安全に仕事や生活するためのいろいろな取り組みや仕組み。**
- **セキュリティはコンピュータを使う人しか関係ない？**
No！ 日常生活を安全にするためのテクニックもセキュリティ。
- **セキュリティを高めるには？ リスク(危険)を減らす。**
- **リスクは資産、脅威、脆弱性からできている。**
- **リスクを構成する三要素のうち、資産と脅威があるだけではリスクは顕在化しない(危険が現実のものとはならない)。脆弱性があるのはじめてリスクが顕在化する。**
- **リスクを減らすには？ 資産、脅威、脆弱性のうちどれかをなくす。まずはどれか一つをなくすようにする。脅威など自分ではどうすることもできないものもある。脆弱性を体系的に減らしていくのが常套手段。**

【例】

「(資産) 家の中に現金(それも大金)がある。」

「(脅威) 世の中に泥棒がいる。」

これだけではリスクは顕在化しないが、

「(脆弱性) 家に鍵をかけ忘れて外出してしまった。」

という事態が重なってリスクが顕在化してしまう。

この例でリスクを減らすためには、まずは

「家の戸締りをきちんとする、鍵をかける・・・。」

という対策をとる(現実的対応策・実現可能)。

「泥棒のいない世の中をつくる。」

という対策もあるが、これは困難(理想的・非現実的対応策)。

セキュリティを高める リスク(脆弱性)を減らす

ペリメータモデルを使って抽象化し、脆弱性を減らす



「内にある資産は基本的に安全である」と仮定する。

「脅威は外からやってくる」と仮定する。

内と外の間境界線(ペリメータライン)を設定し、境界線上の出入りを厳しくチェックすることで脅威の進入を防ぐ。



ペリメータモデル（内は安全、外は危険）

- IT社会・ネットワーク社会特有の考え方？
No！昔からあった。（例）お城、塀、壁、など。
- このモデルさえ適用すれば安心？ No！
内側が信用できるか？ 内側に悪い人がいたら大変！
- それでは内側も疑うようにしたら？ 内側も監視・検閲したら？ 社会全体がぎすぎすする。精神衛生上よくない。

【参考図書】

岡嶋裕史，“セキュリティはなぜ破られるのか 10年使える「セキュリティの考え方」”，講談社ブルーバックス，2006年7月。

情報資産・情報資源に対して**情報セキュリティを確保**するためには

機密性 (Confidentiality) : ネットワーク上やコンピュータ内の情報を不適切な人間には決して見せないようにすること。

完全性 (Integrity) : ネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されないこと。

可用性 (Availability) : ネットワーク上やコンピュータ内の情報や資源 (通信路やコンピュータ) がいつでも利用できること。

証拠性 (Evidential) : 相手に契約書などの文書を偽造・改ざんさせない (偽造・改ざんの有無が確認できる)、不当に事後否認させない。

原本性 (Original) : 情報 (コンピュータプログラム、マルチメディアデータなど) をコピーできない、あるいは不正にコピーされない。

脅威(偶発的)

- 天災(地震、火災、水害、…)
- 故障(HW故障、SW故障、回線障害、…)
- 誤動作(データ入力ミス、誤接続、SWバグ、…)



脅威(意図的)

- 第三者の悪意の行為(不正アクセスなど)
- 取引相手の悪意の行為(取引内容の事後否認、コンテンツの不正コピーなど)

インターネット社会におけるデジタル情報の保護

デジタル情報であることの問題点

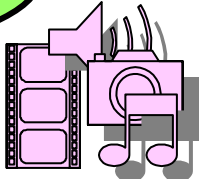
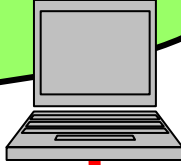
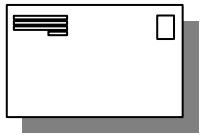
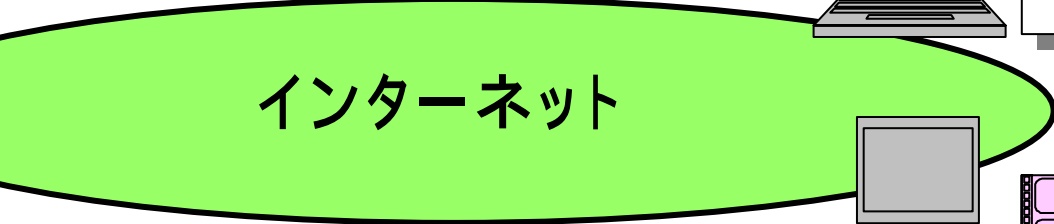
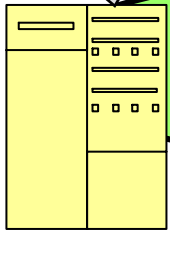
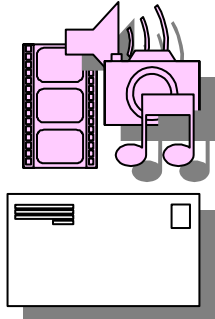
コピーしても劣化しない **コンテンツの不正コピー**
情報の検索・データベース化が容易にできる
個人情報の漏洩、プライバシーの侵害

**アクセス
管理技術**

暗号技術

コンピュータへの不正アクセス(不正侵入)、データの改ざん、破壊

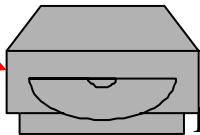
ネットワーク上でのデータの傍受!



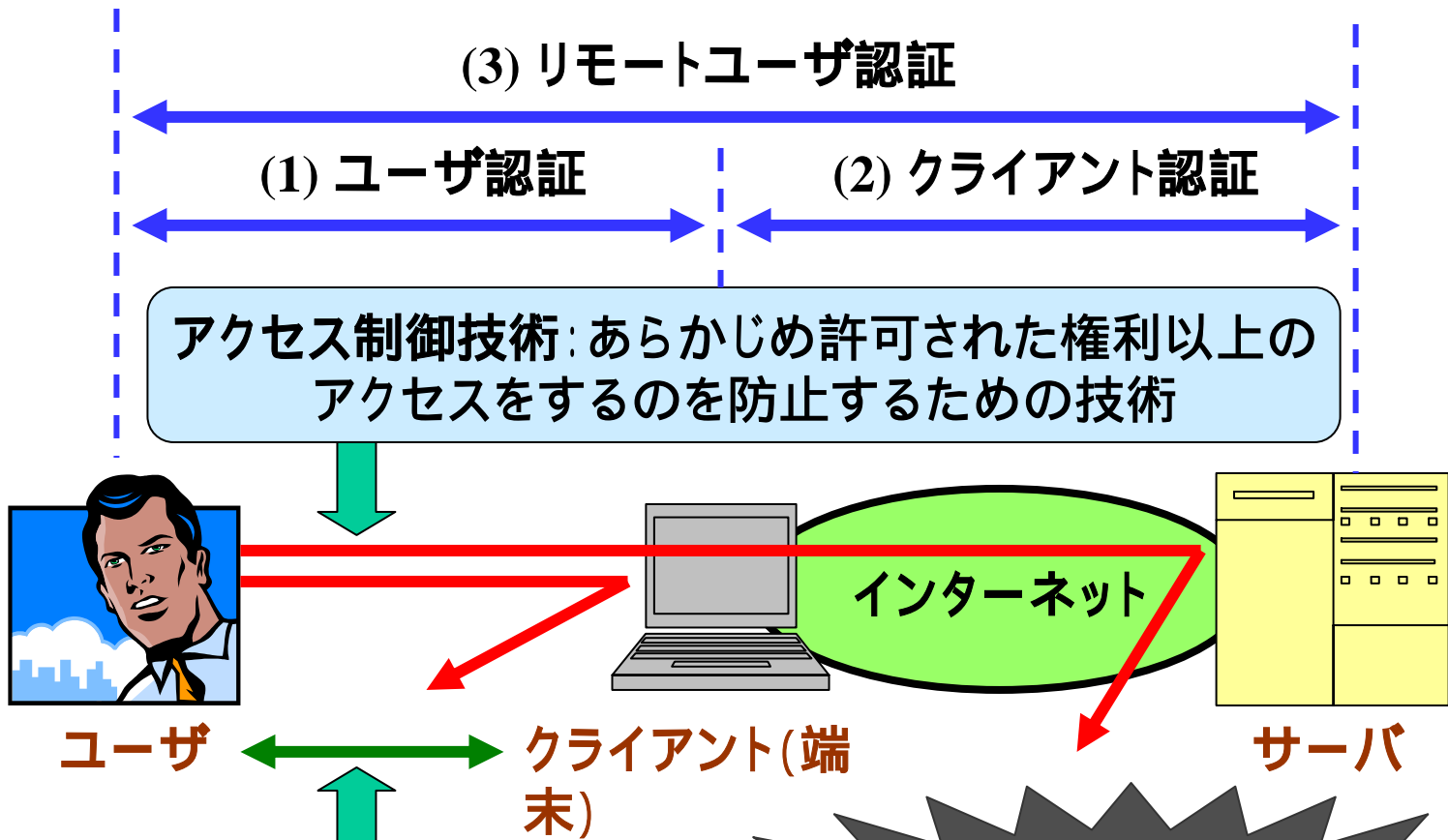
デジタルデータはコピーしても劣化しない!

デジタル接続

電子透かし技術



アクセス管理技術 - インターネット社会のセキュリティを護る技術 -



ユーザ認証技術: 本当に本人かどうかの確認を行う技術
(本人の知識、持ち物、身体的特徴)

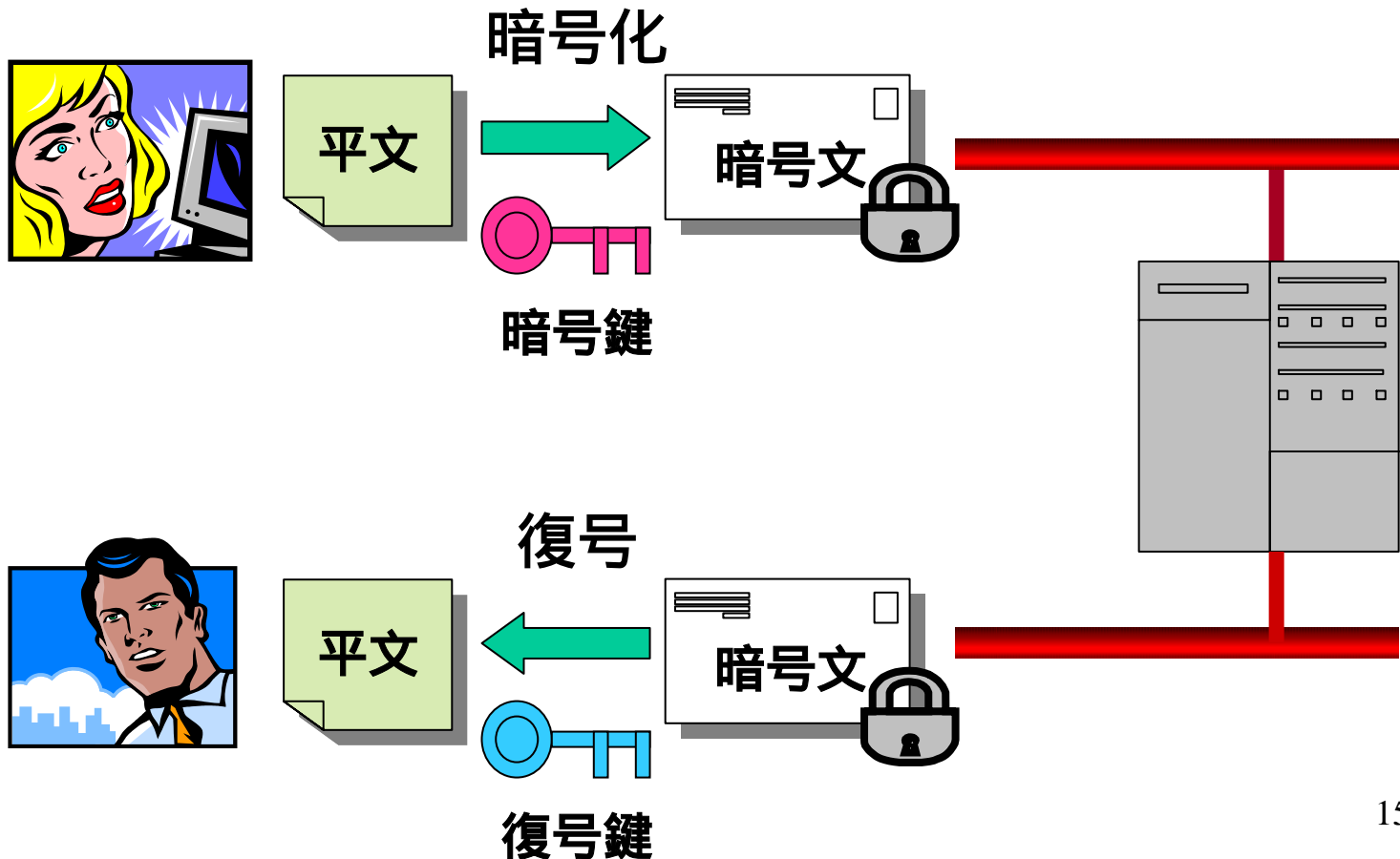
不正アクセス(不正侵入)の方法

1. 他人へのなりすまし
2. セキュリティホール利用

暗号・認証技術 - インターネット社会のセキュリティを護る技術 -

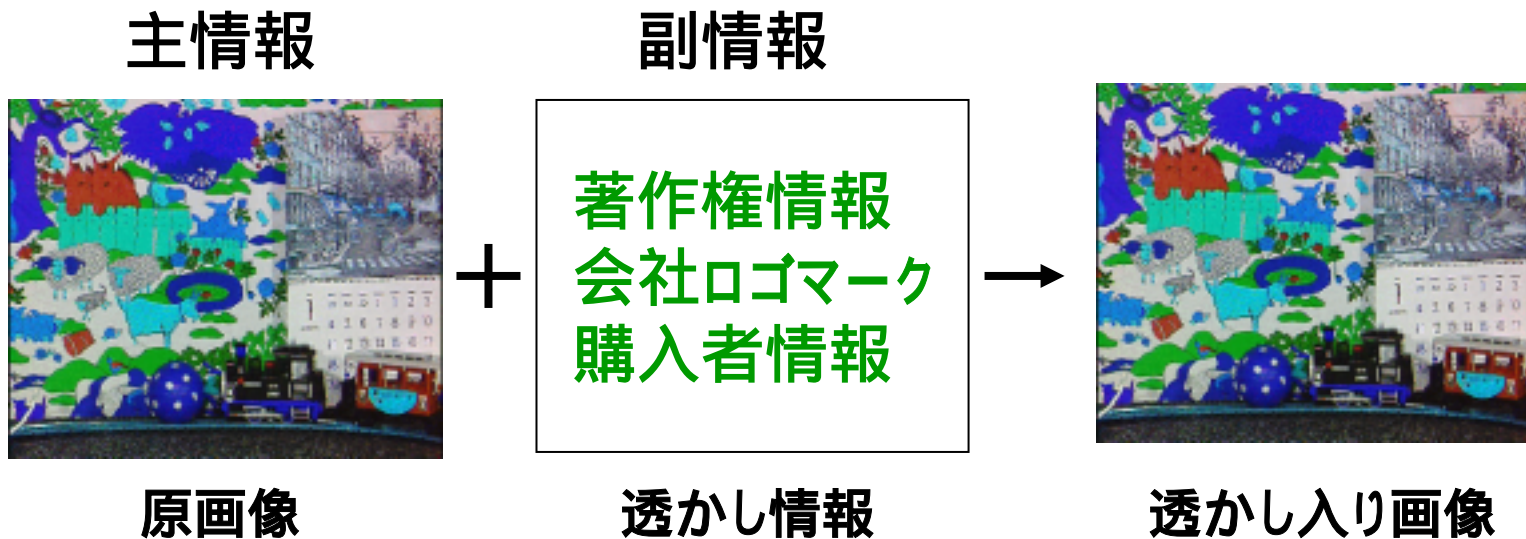
電子メールやクレジットカード情報を他人に知られないようにネットワークで送りたい **暗号による情報の秘匿**

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)**

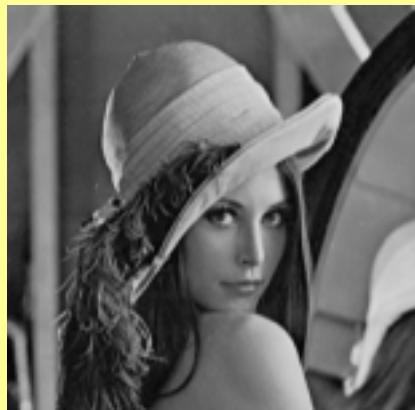


電子透かし(Digital Watermark)技術
- インターネット社会のセキュリティを護る技術 -

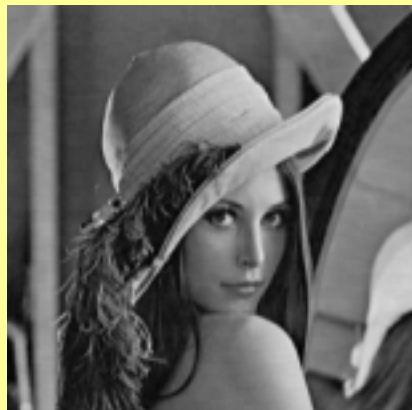
著作権やコピー制御などの情報をデジタルコンテンツの中に、本来のコンテンツ品質を損なわず、人間に知覚されないように埋め込む(忍び込ませる)技術



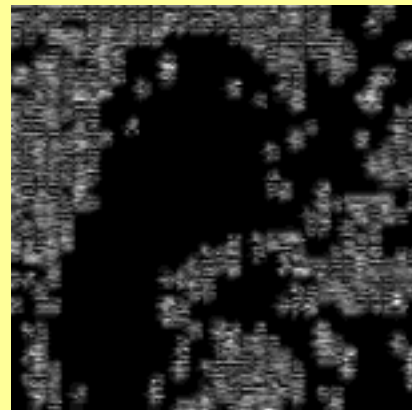
【電子透かしの埋め込み例】



原画像

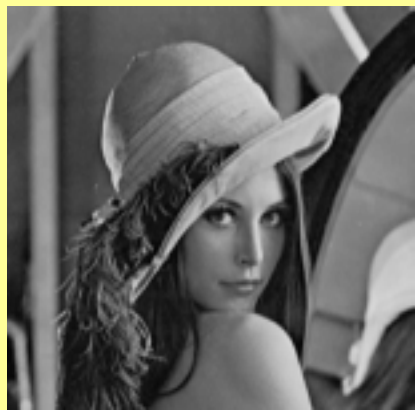


透かし入り画像

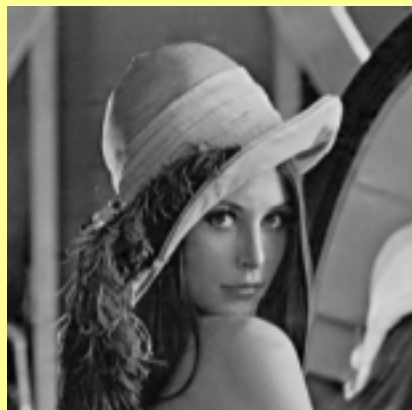


差分画像(32倍強調)

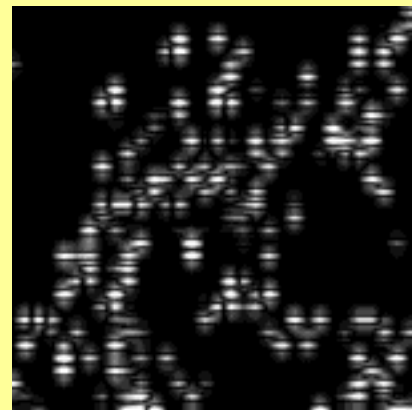
画像の平坦な部分や単調な部分に405ビットの透かし情報が埋め込まれている!



原画像



透かし入り画像

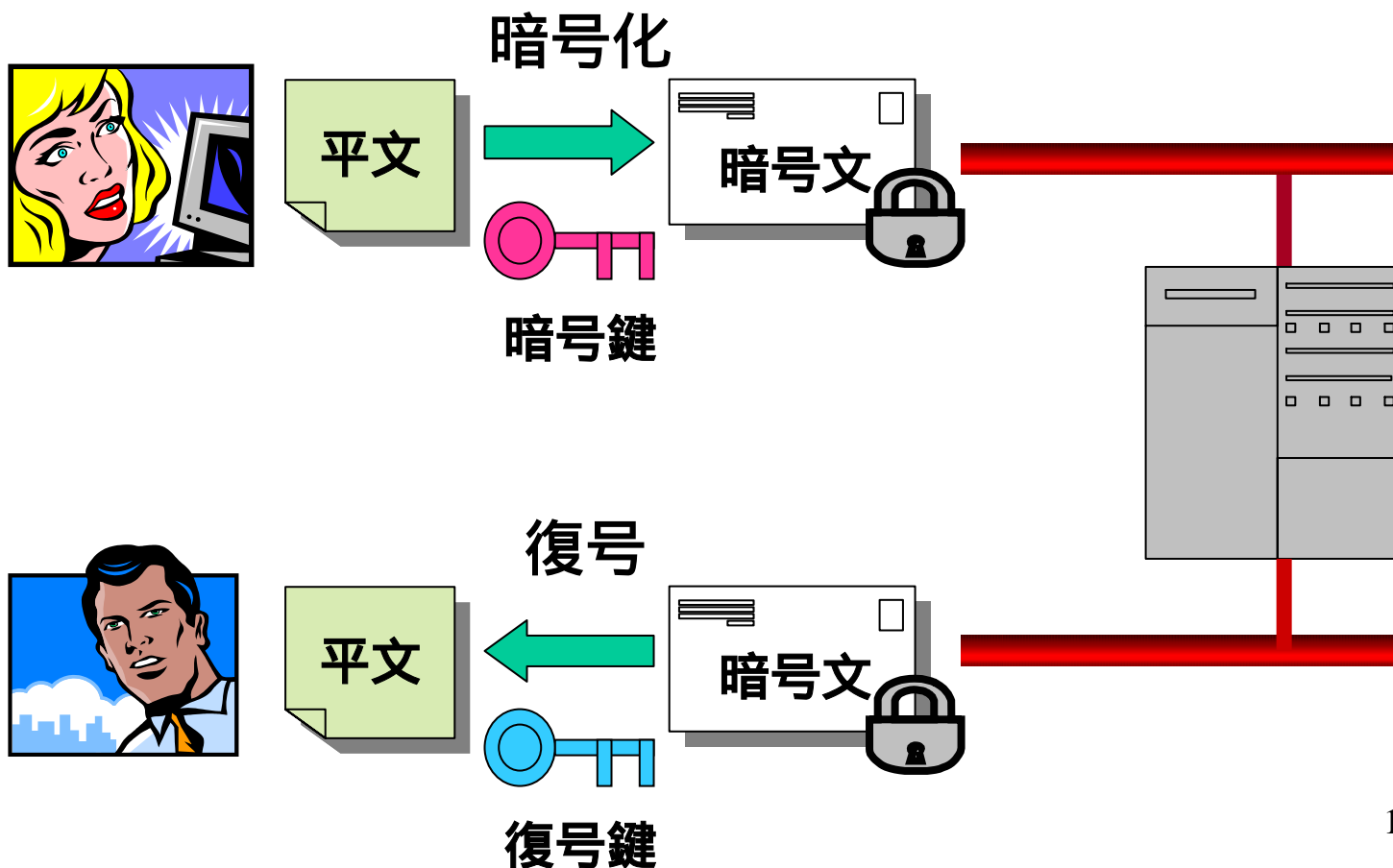


差分画像(32倍強調)

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

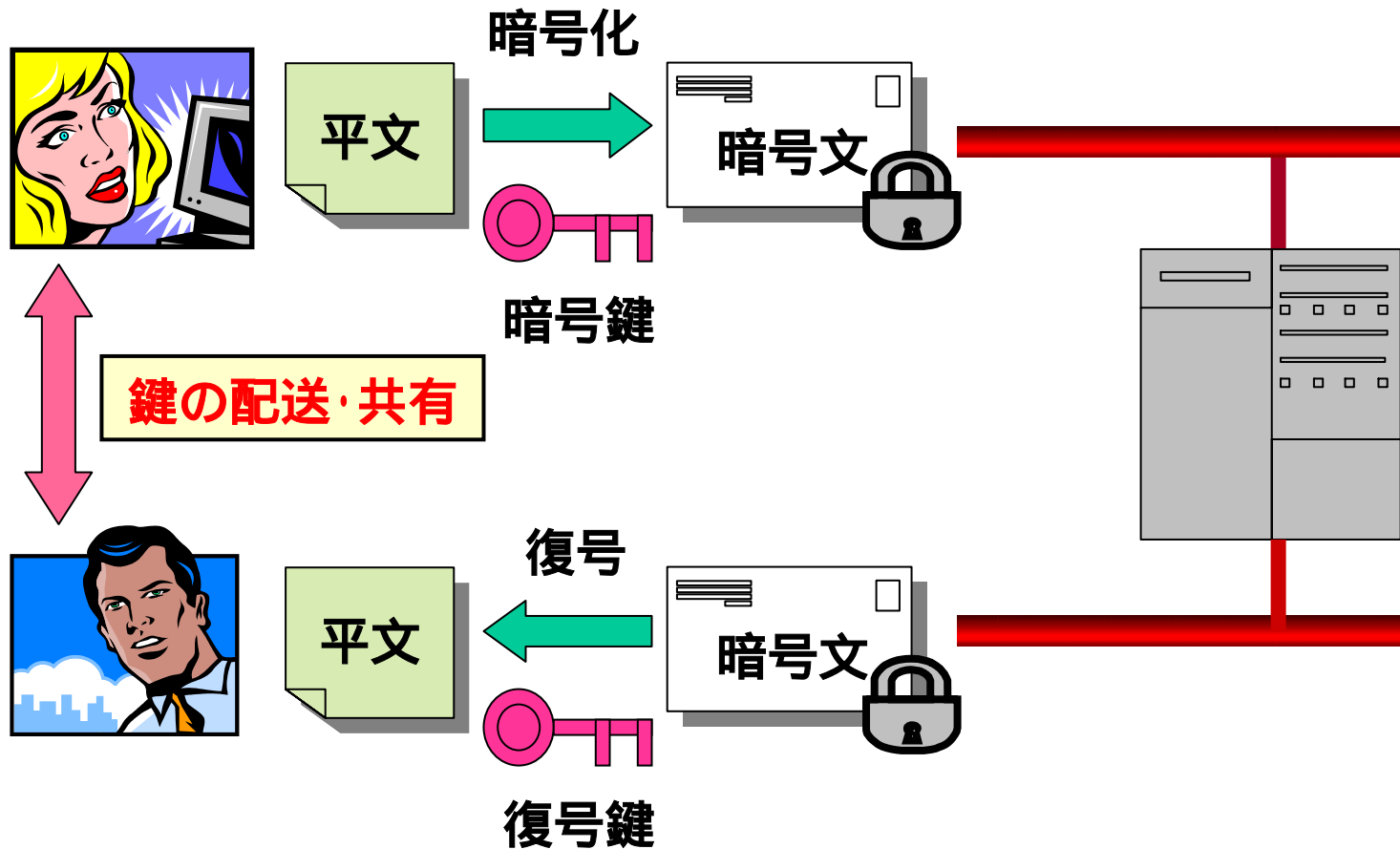
暗号技術 - 暗号のしくみ -

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



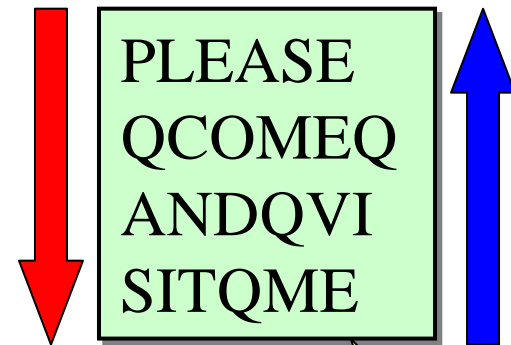
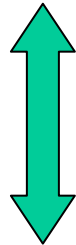


暗号のお話(その1)

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



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: MIYAZKOBCEFGHJLNPQRSTUVWXYZ

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）



125億年

・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)

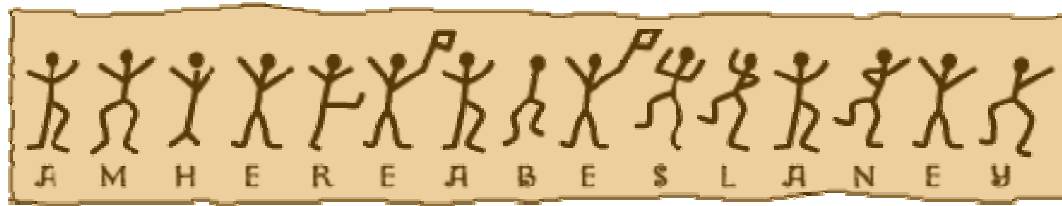
q (0.1) r (6.0) s (6.3) t (9.1) u (2.8) v (1.0) w (2.4) x (0.2)

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;4
8081;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か言った。「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 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 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	T	0		Z	5	
C	1		I	9		O	2		U	7				
D	4		J	8		P	17	t	V	0				
E	15	h	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
F	3	

G	0	
H	0	
I	9	
J	8	r
K	2	
L	2	

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

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

Y	10	a
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	
B	11	
C	1	
D	4	
E	15	h
F	3	

G	0	
H	0	
I	9	
J	8	r
K	2	
L	2	

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

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

Y	10	a
Z	5	

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
C	1	
D	4	n
E	15	h
F	3	

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

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

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

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

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)

↓ 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文字ずつ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。

ヴィジュアル暗号(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)の長さをお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 $26 \times 26 \times 26 = 17,576$ のヴィジュアル暗号(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 $\times 10$!



ネットワーク暗号(大規模ネットワークのための暗号)

- 非常に多くの人を使う、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

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 - 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

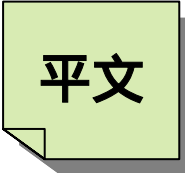
アリスからボブへ暗号化してメールを送る



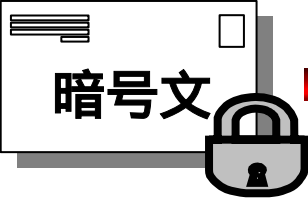
公開鍵一覧表



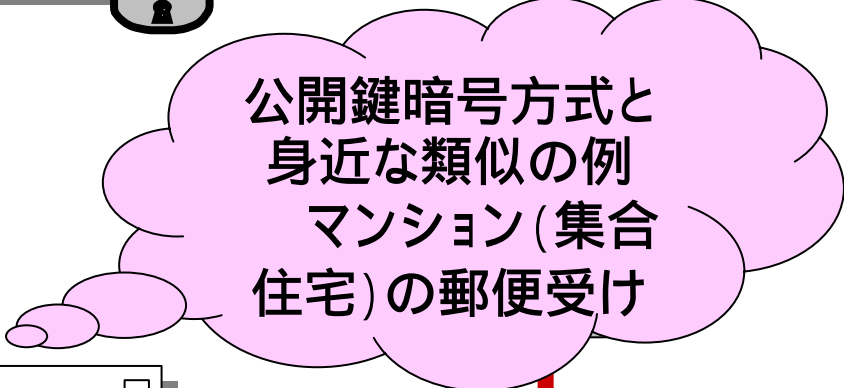
アリス



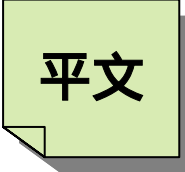
暗号化



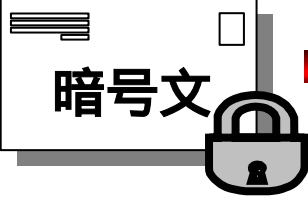
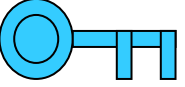
ボブの公開鍵



ボブ



復号



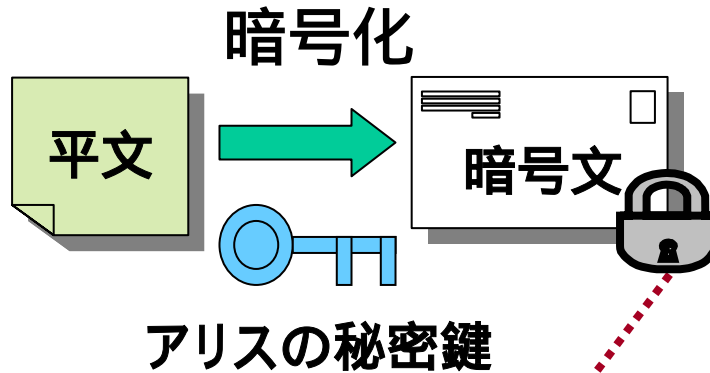
ボブの秘密鍵

公開鍵暗号による情報の秘匿と認証

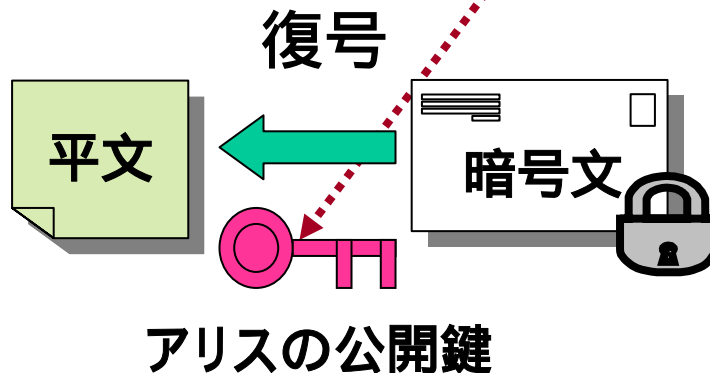
アリスからボブへ暗号化してメールを送る
ボブはアリスからのメールであることを認証
できる



アリス

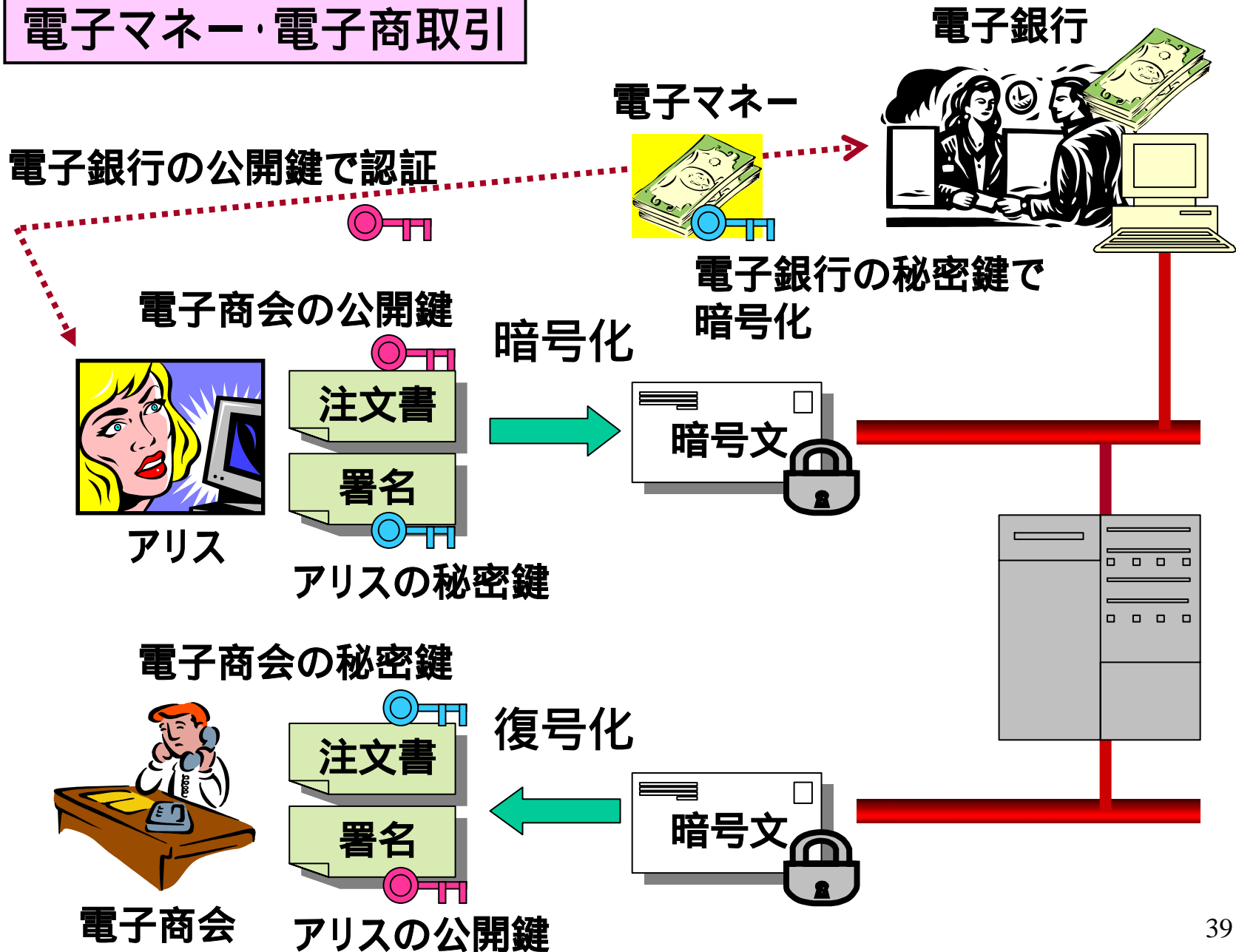


ボブ



公開鍵一覧表

電子マネー・電子商取引



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 - セキュリティを護るために -、米田出版、2000年。
- 今井秀樹、明るい暗号の話 - ネットワーク社会のセキュリティ技術 -、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 - ポストモダンの情報セキュリティ -、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 - マジックプロトコルへの招待 -、講談社ブルーバックス、1995年。
- 西垣 通、IT革命 - ネット社会のゆくえ -、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 - ロゼッタストーンから量子暗号まで -、新潮社、2001年。