知能科学：暗号

平井 慎一

立命館大学 ロボティクス学科

講義の流れ

通信の秘匿

コードトーカー (code talker)

少人数しか理解できない言葉を通信に用いる
「ウインドトーカーズ」：ナバホ語のコードトーカー
薩摩方言の利用

暗号 (cryptography)

シーザー暗号（カエサル）　換字式
ヴィジュネル暗号（ヴィジュネル）　多表式
エニグマ（シェルビウス）　機械式暗号機

量子通信 (quantum cryptography)

量子鍵配送　量子通信により暗号の鍵を送る

暗号

通信文を変換する．

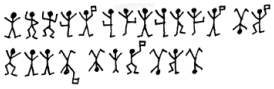
- 送信者と受信者のみが内容を知ることができる．
- 送信者と受信者以外の第三者は内容がわからない．
- 元の文を平文，変換後の文を暗号文とよぶ．

暗号を解読：第三者が何らかの方法で内容を知る．.

暗号

エドガー・アラン・ポー 「黄金虫」

コナン・ドイル「踊る人形」



出典： http://www.alz.jp/221b/holmes/danc.html

江戸川乱歩 「二銭銅貨」

ダン・ブラウン「ダ・ヴィンチ・コード」

換字式暗号

換字式（かえじしき）暗号 (substitution cipher)
平文の文字を，ある規則に基づいて変換する．

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;‡?;*

出典：エドガー・アラン・ポー 「黄金虫」
https://ja.wikipedia.org/wiki/黄金虫_(小説)

換字式暗号

平文

A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.

暗号文

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;‡?;*

出典：エドガー・アラン・ポー 「黄金虫」
https://ja.wikipedia.org/wiki/黄金虫_(小説)

換字式暗号

鍵 (key)

a	b	c	d	e	f	g	h	i	j	k	l	m	n
5	2	—	†	8	1	3	4	6			0	9	*
o	p	q	r	s	t	u	v	w	x	y	z		
‡	.		(	)	;	?	¶			:			

換字式暗号の解読

頻度分布攻撃

各記号の頻度

8	;	4	‡	)	*	5	6	(	···
33	26	19	16	16	13	12	11	10	···

換字式暗号の解読

頻度分布攻撃

各記号の頻度

8	;	4	‡	)	*	5	6	(	···
33	26	19	16	16	13	12	11	10	···

記号 ‘8’ を 文字 ‘e’ と推測

3 連記号列の頻度

;48	)4 ‡	*;4	8 † 8	‡ (;	···
7	4	3	3	3	···

記号列 ‘;48’ を文字列 ‘the’ と推測

記号 ‘;’ を 文字 ‘t’ と推測

記号 ‘4’ を 文字 ‘h’ と推測

換字式暗号の解読

頻度分布攻撃

各記号の頻度

8	;	4	‡	)	*	5	6	(	···
33	26	19	16	16	13	12	11	10	···

記号 ‘8’ を 文字 ‘e’ と推測

暗号の解読

多表式：複数の換字表を順番に用いる
鍵語でどの換字表を用いるかを指定する．頻度分析攻撃に強い．

ヴィジュネル暗号：カシスキーテスト攻撃
ヴィジュネル暗号の周期性に着目
鍵語の桁数が少ない場合に有効

エニグマ：鍵語の長さ 105456

エニグマの初期型の解読（周期性に着目）
レイェフスキ，ジガルスキ，ルジツキ（ポーランド）
解読機械ボンバとエニグマの模擬機械を接続：解読の高速化

政治情勢の悪化：ポーランドの技術をイギリスに伝える
ボンベによるエニグマの解読

換字式暗号の解読

頻度分布攻撃

各記号の頻度

8	;	4	‡	)	*	5	6	(	···
33	26	19	16	16	13	12	11	10	···

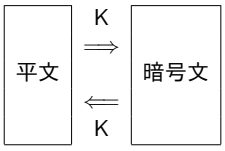
記号 ‘8’ を 文字 ‘e’ と推測

3 連記号列の頻度

;48	)4 ‡	*;4	8 † 8	‡ (;	···
7	4	3	3	3	···

暗号

鍵 (key)



換字式暗号の解読

頻度分布攻撃

各記号の頻度

8	;	4	‡	)	*	5	6	(	···
33	26	19	16	16	13	12	11	10	···

記号 ‘8’ を 文字 ‘e’ と推測

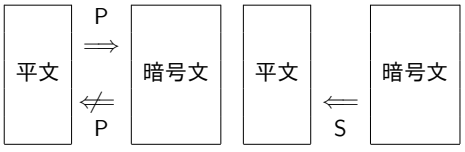
3 連記号列の頻度

;48	)4 ‡	*;4	8 † 8	‡ (;	···
7	4	3	3	3	···

記号列 ‘;48’ を文字列 ‘the’ と推測

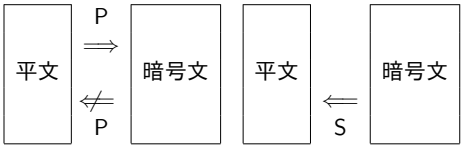
公開鍵暗号

公開鍵 (public key)　　秘密鍵 (secret key)



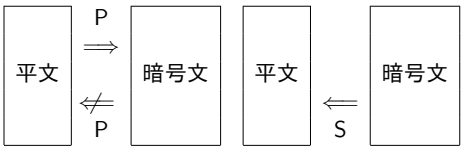
公開鍵暗号

公開鍵 (public key)　　秘密鍵 (secret key)



公開鍵暗号

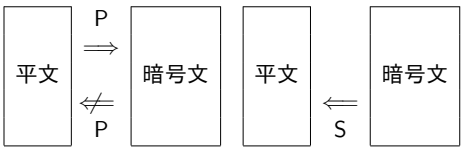
公開鍵 (public key)　　秘密鍵 (secret key)



受信者：P と S を作成．P を公開

公開鍵暗号

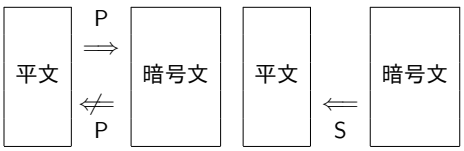
公開鍵 (public key)　　秘密鍵 (secret key)



受信者：P と S を作成．P を公開
送信者：P を使って平文 x を暗号文 y に変換　$y = P(x)$
　　暗号文 y を受信者に送信

公開鍵暗号

公開鍵 (public key)　　秘密鍵 (secret key)



受信者：P と S を作成．P を公開
送信者：P を使って平文 x を暗号文 y に変換　$y = P(x)$
　　暗号文 y を受信者に送信
受信者：S を使って暗号文 y を平文 x に復元　$x = S(y)$

公開鍵暗号

公開鍵 (public key)　　秘密鍵 (secret key)

受信者：P と S を作成．P を公開
送信者：P を使って平文 x を暗号文 y に変換　$y = P(x)$
　　暗号文 y を受信者に送信
受信者：S を使って暗号文 y を平文 x に復元　$x = S(y)$
第三者：S を知らないので暗号文 y を平文に復元できない

公開鍵暗号

公開鍵暗号の概念：ディフィー，ヘルマン，マークル
　　Diffie, Hellman, Merkle
2015 年チューリング賞

RSA 暗号：リベスト，シャミア，エーデルマン
　　Rivest, Shamir, Adelman
公開鍵暗号の実現
2002 年チューリング賞

素因数分解

素数 p と q　$\underset{\text{素因数分解}}{\overset{\text{積}}{\rightleftharpoons}}$　$n = pq$

積の計算：　容易
素因数分解：　困難

p：10 桁，q：10 桁　$\underset{\text{困難}}{\overset{\text{容易}}{\rightleftharpoons}}$　$n = pq$：20 桁

RSA 暗号

受信者
- 素数 p と q を選ぶ．$n = pq$
- $(p-1)(q-1)$ と素な自然数 e を選ぶ．
  互いに素：　最大公約数が 1
- ed を $(p-1)(q-1)$ で割った余りが 1 となる d を選ぶ．
- 公開鍵 $\mathrm{P} = (e, n)$　　秘密鍵 $\mathrm{S} = d$

RSA 暗号

受信者
- 素数 p と q を選ぶ．$n = pq$
- $(p-1)(q-1)$ と素な自然数 e を選ぶ．
  互いに素： 最大公約数が 1
- ed を $(p-1)(q-1)$ で割った余りが 1 となる d を選ぶ．
- 公開鍵 $\mathrm{P} = (e, n)$　秘密鍵 $\mathrm{S} = d$

送信者
- 平文 x $(< n)$
- 公開鍵を使って暗号文 $y = x^e \bmod n$ を作成
  （mod n は n で割った余りを意味する）

RSA 暗号

受信者
- 素数 p と q を選ぶ．$n = pq$
- $(p-1)(q-1)$ と素な自然数 e を選ぶ．
  互いに素： 最大公約数が 1
- ed を $(p-1)(q-1)$ で割った余りが 1 となる d を選ぶ．
- 公開鍵 $\mathrm{P} = (e, n)$　秘密鍵 $\mathrm{S} = d$

送信者
- 平文 x $(< n)$
- 公開鍵を使って暗号文 $y = x^e \bmod n$ を作成
  （mod n は n で割った余りを意味する）

受信者
- 秘密鍵を使って $y^d \bmod n$ を計算．これが x に一致する．

RSA 暗号

受信者
- $p = 7$ と $q = 11$ を選ぶ．$n = pq = 77$
- $(p-1)(q-1) = 60$ と素な自然数 $e = 13$ を選ぶ．
  $\mathrm{GCD}\,(60, 13) = 1$
- $d = 37$ を選ぶ．$\mathtt{rem}\,(ed = 481, (p-1)(q-1) = 60) = 1$
- 公開鍵 $\mathrm{P} = (e, n)$　秘密鍵 $\mathrm{S} = d$

送信者
- 平文 $x = 15$ (< 77)
- 暗号文 $y = 15^{13} \bmod 77 = \mathtt{rem(15\hat{}13,\ 77)} = 64$
  暗号文 y を送信

受信者
- $64^{37} \bmod 77 = \mathtt{rem(64\hat{}37,\ 77)} = 15$ が平文に一致

RSA 暗号

秘密鍵 d

$\Uparrow$

e

$\Uparrow$

p と q

$\Uparrow$

n を素因数分解

素因数分解を効率的に解くアルゴリズムが存在しないことが前提
量子計算では効率的に解くことが可能?

まとめ

暗号
- 換字式暗号
- 鍵

公開鍵暗号
- RSA 暗号
- 素因数分解