公開鍵暗号という革命

セキュリティを支える数学の世界

目次

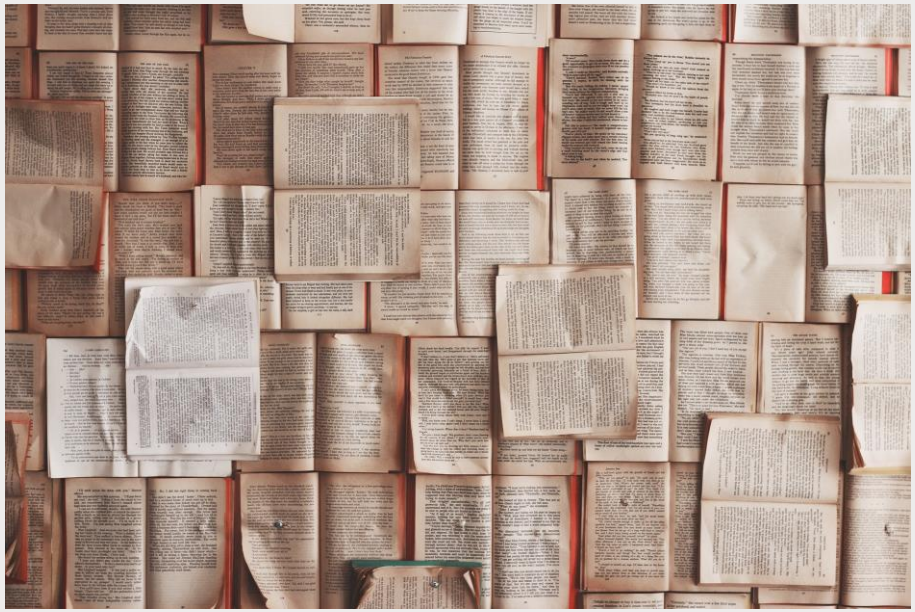
- 身の回りの暗号技術
- 暗号技術の歩み
- 共通鍵暗号とその問題点
- 公開鍵暗号
- modの世界で公開鍵暗号を実現する
- ハイブリッド暗号

目次

- 身の回りの暗号技術
- 暗号技術の歩み
- 共通鍵暗号とその問題点
- 公開鍵暗号
- modの世界で公開鍵暗号を実現する
- ハイブリッド暗号

“暗号”といえば…

イミテーション
ゲーム



エニグマ

身近な暗号技術


アーカイブユーティリティ
“image.png”のパスワードを入力してください。
パスワード:
キャンセル
OK
大阪大学附属図書館 - 理工学図書
保護された通信
https://www.library.osaka-u.ac.
大阪大学附属図
OSAKA
メモ
このトークルームのメッセージは 暗号化されて安全です。

目次

- 身の回りの暗号技術
- 暗号技術の歩み
- 共通鍵暗号とその問題点
- 公開鍵暗号
- modの世界で公開鍵暗号を実現する
- ハイブリッド暗号

暗号のはじまり

時は紀元前，あなたは宮殿に仕える衛兵
怪しげなメモ書きを見つけた

Igjj igle rmkmppmu

- 特定の知識を持った人にのみ伝わる
- 第3者には元の内容がわからない

暗号のはじまり

- 特定の人（自分の仲間）にだけ伝えたい

明日9時に駅前 ⟹ “焼肉定食”

明日3時に駅前 ⟹ “寿司食べ放題”

今日9時に学校 ⟹ “スイーツパラダイス”

今日3時に学校 ⟹ “ハンバーグ”

暗号のはじまり

- 特定の人（自分の仲間）にだけ伝えたい

明日/9時に/駅前 ⟹ “焼肉””寿司”パスタ”

明日/3時に/駅前 ⟹ “焼肉””米””パスタ”

今日/9時に/学校 ⟹ “カレー””寿司””パン”

今日/9時に/駅前 ⟹ “カレー””寿司””パスタ”

暗号のはじまり

- 特定の人（自分の仲間）にだけ伝えたい

あ → い　　え → お

い → う　　お → か

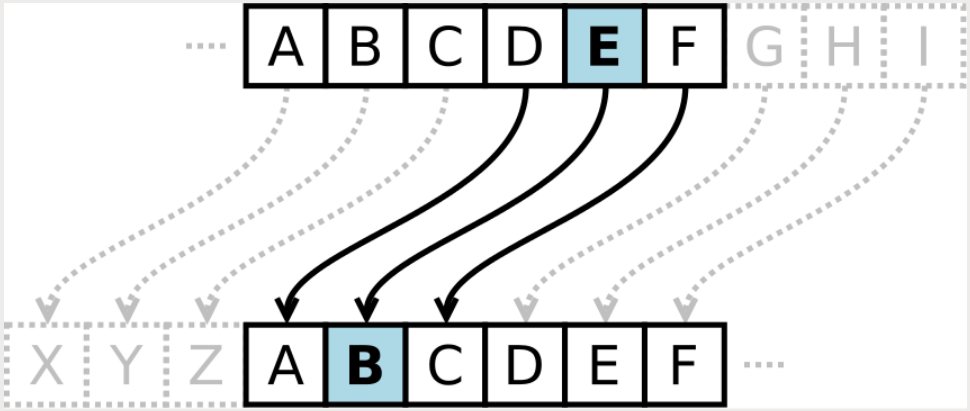
う → え　　か → き　……

こんにちは → “さあぬつひ”

“かにきせうち” → おなかすいた

シーザー暗号

- 古代ローマのユリウス・カエサルが使用
  辞書順に3文字戻して秘密文章を記した



“F XJ ERKDOV” → I AM HUNGRY

シーザー暗号

Hello world

k 文字
戻す

Uryyb Jbeyq

Uryyb Jbeyq

Uryyb Jbeyq

？？？

Uryyb Jbeyq

k 文字
進める

Hello world

シーザー暗号を解く

Igjj igle rmkmppmu

- たかだか26通りしかない（鍵空間が小さい）

igjj igle rmkmppmu
Jhkk jhmf snlnqqnv
kill king tomorrow
ljmm ljoh upnpsspx
mknn mkpi vqoqttqy
nloo nlqj wrpruurz
ompp omrk xsqsvvsa
pnqq pnsl ytrtwwtb
qorr qotm zusuxxuc
rpss rpun avtvyyvd
sqtt sqvo bwuwzzwe
truu trwp cxvxaaxf
usvv usxq dywybbyg
vtww vtyr ezxzcczh
wuxx wuzs fayaddai
xvyy xvat gbzbeebj
ywzz ywbu hcacffck
zxaa zxcv idbdggdl
aybb aydw jecehhem
bzcc bzex kfdfiifn
cadd cafy lgegjjgo
dbee dbgz mhfhkkhp
ecff echa nigilliq
fdgg fdib ojhjmmjr
gehh gejc pkiknnks
hfii hfkd qljloolt

より強い暗号へ

- アルファベットの対応表を作る
  26! 通りの変換
- ASCIIコードを使う

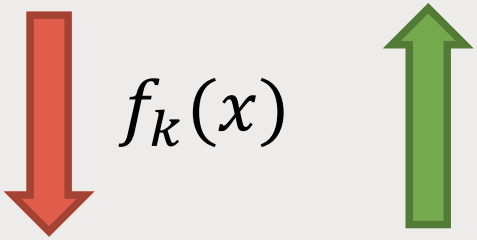
0		1		2		3		4		5		6		7	
8		9		10		11		12		13		14		15	
16		17		18		19		20		21		22		23	
24		25		26		27		28		29		30		31	
32		33	!	34	"	35	#	36	$	37	%	38	&	39	'
40	(	41	)	42	*	43	+	44	,	45	-	46	.	47	/
48	0	49	1	50	2	51	3	52	4	53	5	54	6	55	7
56	8	57	9	58	:	59	;	60	<	61	=	62	>	63	?
64	@	65	A	66	B	67	C	68	D	69	E	70	F	71	G
72	H	73	I	74	J	75	K	76	L	77	M	78	N	79	O
80	P	81	Q	82	R	83	S	84	T	85	U	86	V	87	W
88	X	89	Y	90	Z	91	[	92	¥	93	]	94	^	95	_
96	`	97	a	98	b	99	c	100	d	101	e	102	f	103	g
104	h	105	i	106	j	107	k	108	l	109	m	110	n	111	o
112	p	113	q	114	r	115	s	116	t	117	u	118	v	119	w
120	x	121	y	122	z	123	{	124	|	125	}	126	~	127	

鍵空間がより大きくなる

より強い暗号へ

- ASCIIコードを使う

H	e	l	l	o	!
72	101	108	108	111	33



鍵 k 

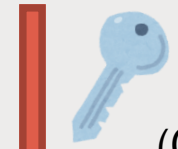
$	P	@	b	9	g
36	80	64	98	57	103

目次

- 身の回りの暗号技術
- 暗号技術の歩み
- **共通鍵暗号とその問題点**
- 公開鍵暗号
- modの世界で公開鍵暗号を実現する
- ハイブリッド暗号

共通鍵暗号

こんにちは
(0110101.....)



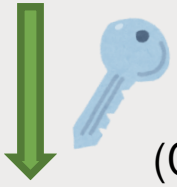
鍵 k
(0010.....)

0a7?+ja¥
(1101001.....)

0a7?+ja¥

？？

0a7?+ja¥
(1101001.....)



鍵 k
(0010.....)

こんにちは
(0110101.....)

鍵 k はどうやって交換した？？？

鍵の共有

鍵 k
(0110101.....)

鍵 k'
(0010.....)

jf1e3@&f
(1101001.....)

jf1e3@&f

？？

jf1e3@&f
(1101001.....)

鍵 k'
(0010.....)

鍵 k
(0110101.....)

鍵 k' はどうやって交換した？？？

共通鍵暗号の問題点

- 暗号化・復号に同じ鍵を使う
- 鍵を安全に共有する手段がない

- 鍵を共有せずに暗号化・復号できないか？
- 暗号化・復号に使う鍵が異なれば良い？

“公開鍵暗号”という概念の誕生

1960年ごろ

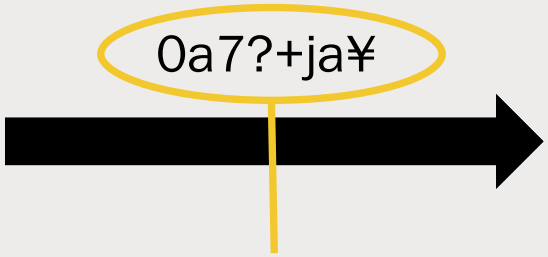
目次

- 身の回りの暗号技術
- 暗号技術の歩み
- 共通鍵暗号とその問題点
- **公開鍵暗号**
- modの世界で公開鍵暗号を実現する
- ハイブリッド暗号

公開鍵暗号

こんにちは

0a7?+ja¥



0a7?+ja¥

こんにちは

0a7?+ja¥

こんにちは

公開鍵暗号

- 暗号化・復号に使う鍵が異なる

  公開鍵  で暗号化したものは

  秘密鍵  でしか復号できない

- 公開鍵から秘密鍵を簡単に求められない

そんな都合のいい話があるのか？？

あるんです

- 主な公開鍵暗号

RSA暗号：素因数分解問題

ElGamal暗号：有限体上の離散対数問題

楕円曲線暗号：楕円曲線上の離散対数問題

目次

- 身の回りの暗号技術
- 暗号技術の歩み
- 共通鍵暗号とその問題点
- 公開鍵暗号
- modの世界で公開鍵暗号を実現する
- ハイブリッド暗号

Mod演算

- $a \equiv b \mod n$

  aをnで割った余りがb　$a = kn + b$

  a, bはnを法として合同

  int b = a%n と書いたことがあるのでは

- 具体例

  35 ≡ 2 mod 33　　79 ≡ 13 mod 33

  35 + 79 ≡ 2 + 13 ≡ 15 mod 33

  35 * 79 ≡ 2 * 13 ≡ 26 mod 33

べき乗算を考える

- 33を法として（mod 33）

$2^1 \equiv 2$　　$2^6 \equiv 64 \equiv 31$　　$2^{11} \equiv 2$

$2^2 \equiv 4$　　$2^7 \equiv 128 \equiv 29$　　$2^{12} \equiv 4$

$2^3 \equiv 8$　　$2^8 \equiv 256 \equiv 25$　　$2^{13} \equiv 8$

$2^4 \equiv 16$　　$2^9 \equiv 512 \equiv 17$　　$2^{14} \equiv 16$

$2^5 \equiv 32$　　$2^{10} \equiv 1024 \equiv 1$　　⋮

- 何乗かすれば元の数字に戻る？

もっと考える

■ 33を法として（mod 33）

$14^1 \equiv 14$

$14^2 \equiv 196 \equiv 31$

$14^3 \equiv$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
13	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13
14	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14
15	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15
16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16
17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18
19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32

公開鍵暗号へ

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10

復号 e乗

暗号化 d乗

秘密鍵 k_{sec}

公開鍵 k_{pub}

mod 33 なら，$k_{pub} = 3,\ k_{sec} = 7$

公開鍵暗号

公開鍵
k_{pub}

こんにちは

k_{pub}

0a7?+ja¥

0a7?+ja¥

0a7?+ja¥

0a7?+ja¥

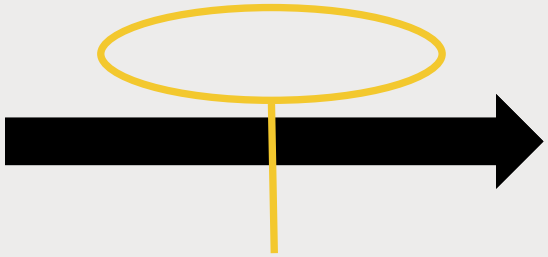
秘密鍵
k_{sec}

こんにちは

こんにちは

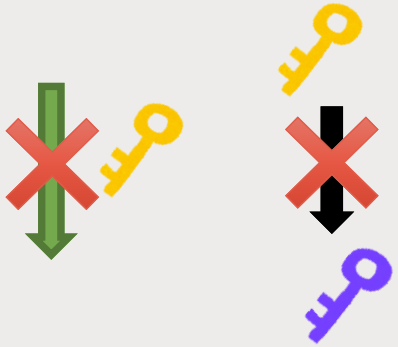
RSA暗号

mod 33 で 3乗して
送ってください



mod 33で
3乗する

mod 33で
7乗する



公開鍵から秘密鍵を求められない？

mod 33 で  $k_{pub} = 3$   $k_{sec} = 7$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5

$33 = 3 \times 11$ $2 \times^{32} 10 + 1 = 21$

mod $N = P \times Q$ なら $(P-1)(Q-1)+1$

（P, Q は素数）

素因数分解

→ 困難

$6887 = 71 \times 97$

N = 2048 bit 600桁くらい

目次

- 身の回りの暗号技術
- 暗号技術の歩み
- 共通鍵暗号とその問題点
- 公開鍵暗号という発想
- modの世界で公開鍵暗号を実現する
- ハイブリッド暗号

ハイブリット暗号

- 公開鍵暗号は共通鍵暗号に比べて
  実行時間がかかる

- 公開鍵暗号で共通鍵を共有して
  以降は共通鍵暗号で暗号化すればよい！
  → ハイブリッド暗号

ハイブリッド暗号

0a7?+ja¥

こんにちは

T35k@m0

0a7?+ja¥

T35k@m0

公開鍵

k_{pub}

0a7?+ja¥

秘密鍵

k_{sec}

T35k@m0

こんにちは

まとめ

- 暗号技術にお世話にならない日はない！
- 鍵空間が小さければ総当たりで解ける！
- 共通鍵暗号は鍵共有が問題！
- 公開鍵暗号は同じ鍵を共有する必要がない！
- 公開鍵暗号は数学的難問に支えられている！