公開鍵暗号

ネットワークと情報セキュリティ5

菊池浩明

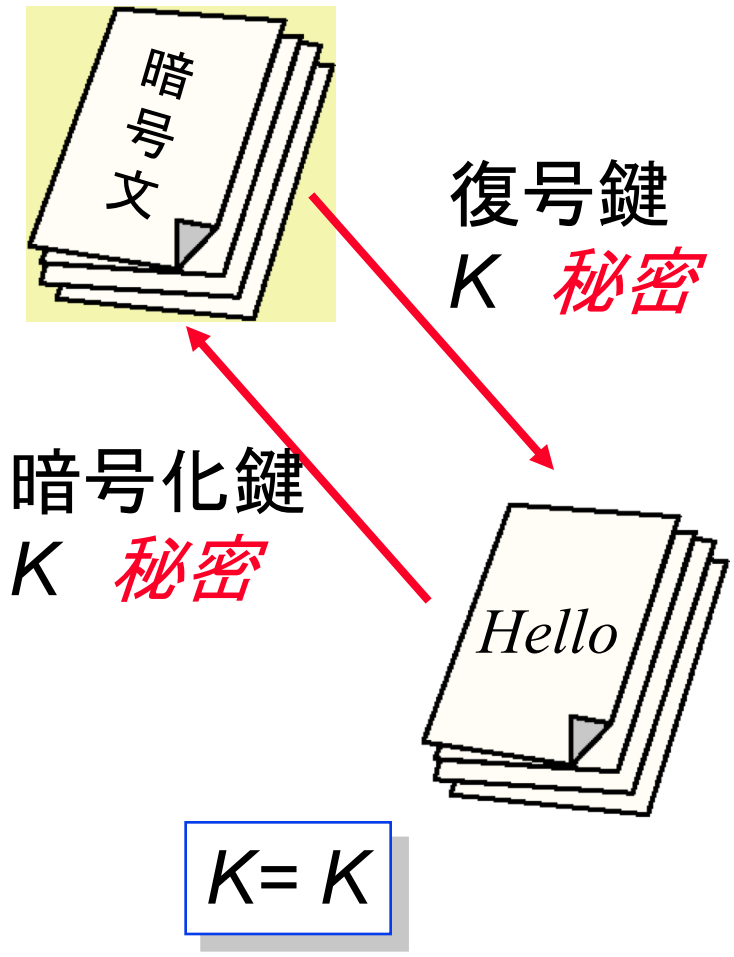
Contents

- 5.1 公開鍵アルゴリズムの基礎
  - 整数論の基礎
- 5.2 DH鍵共有
- 5.3 RSA暗号
  - (5.4 ディジタル署名は次回)

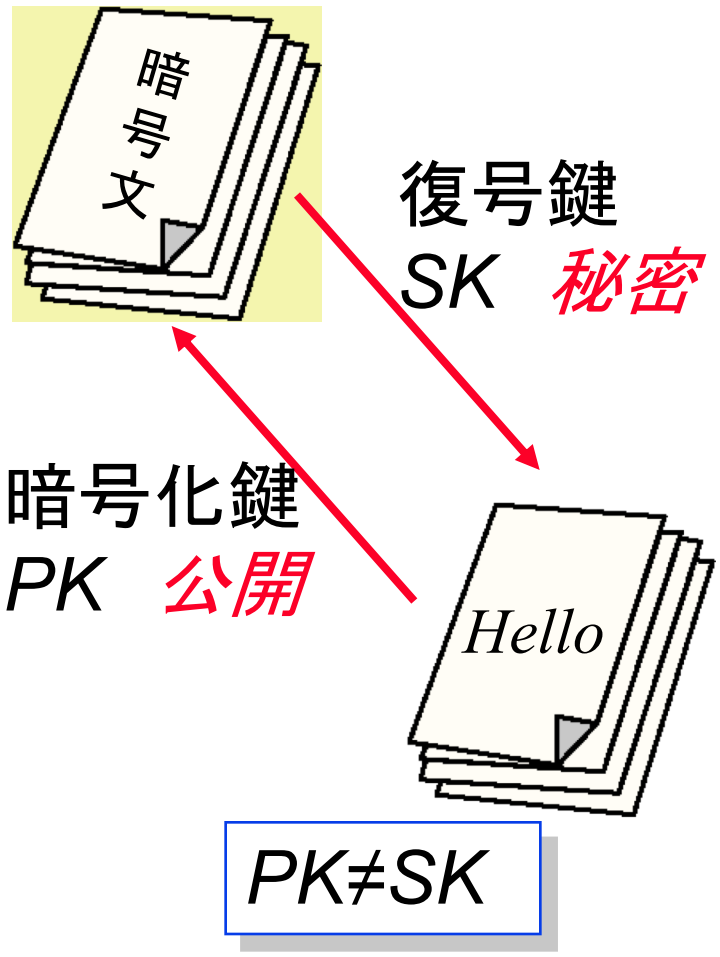
公開鍵アルゴリズムの基礎

公開鍵暗号

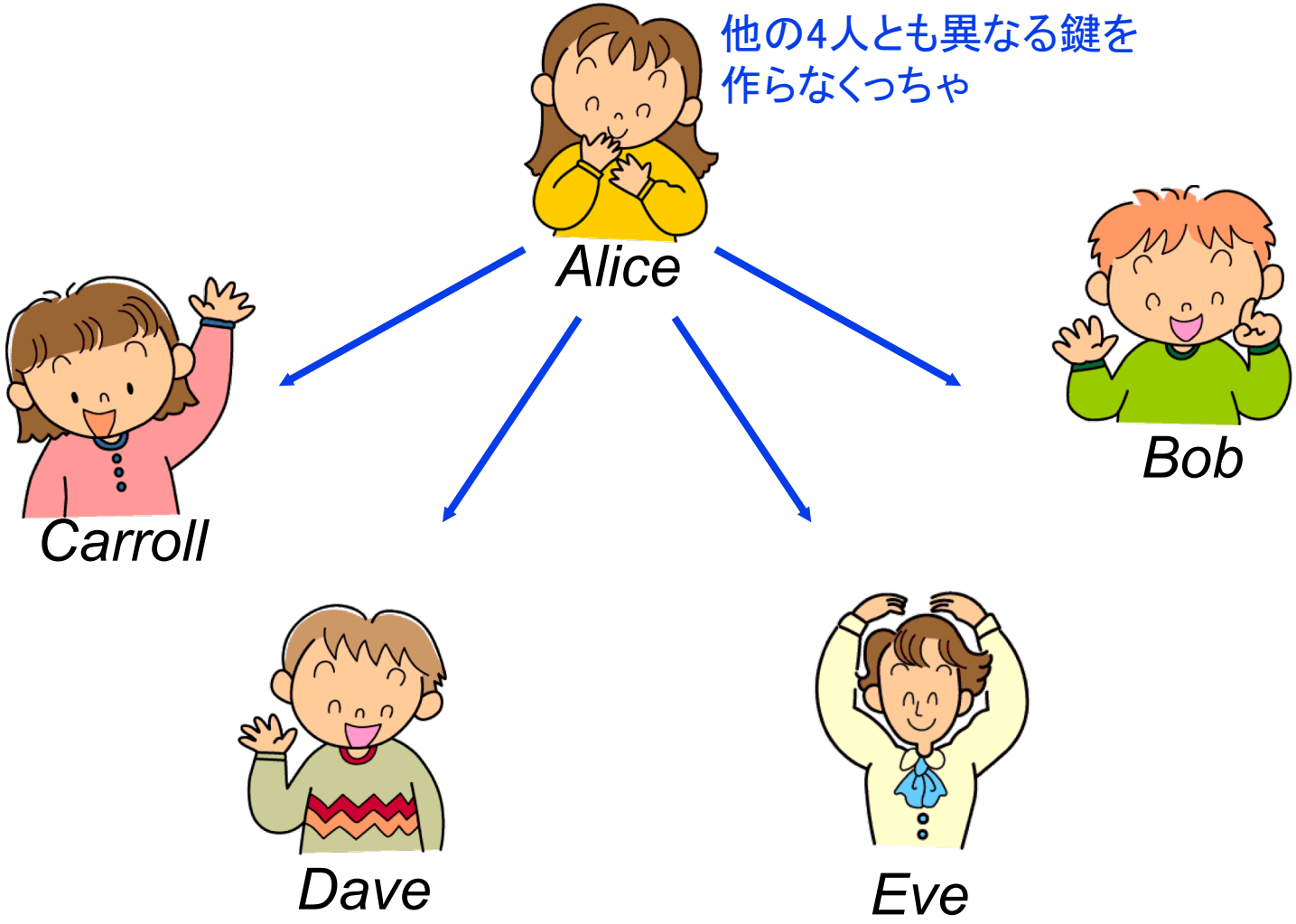
- 共通鍵暗号



- 公開鍵暗号

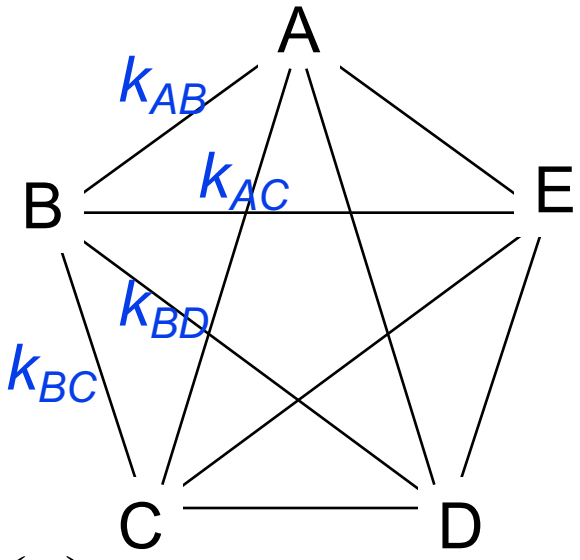


問題「全部で何個の共通鍵が必要？」



スケーラビリティ（大規模拡張性）

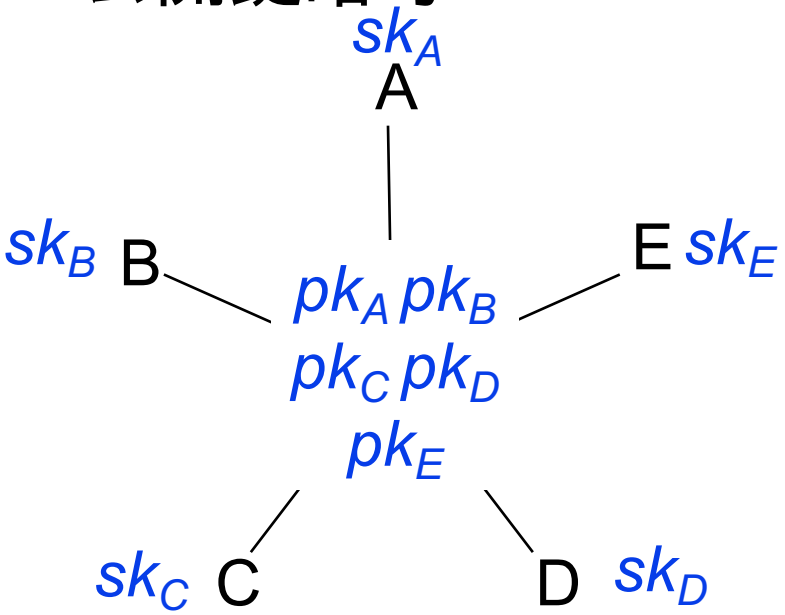
- 共通鍵暗号



$$\binom{n}{2} = \frac{n(n-1)}{2} = O(n^2)$$

n=5の時: 5*4/2 = 10

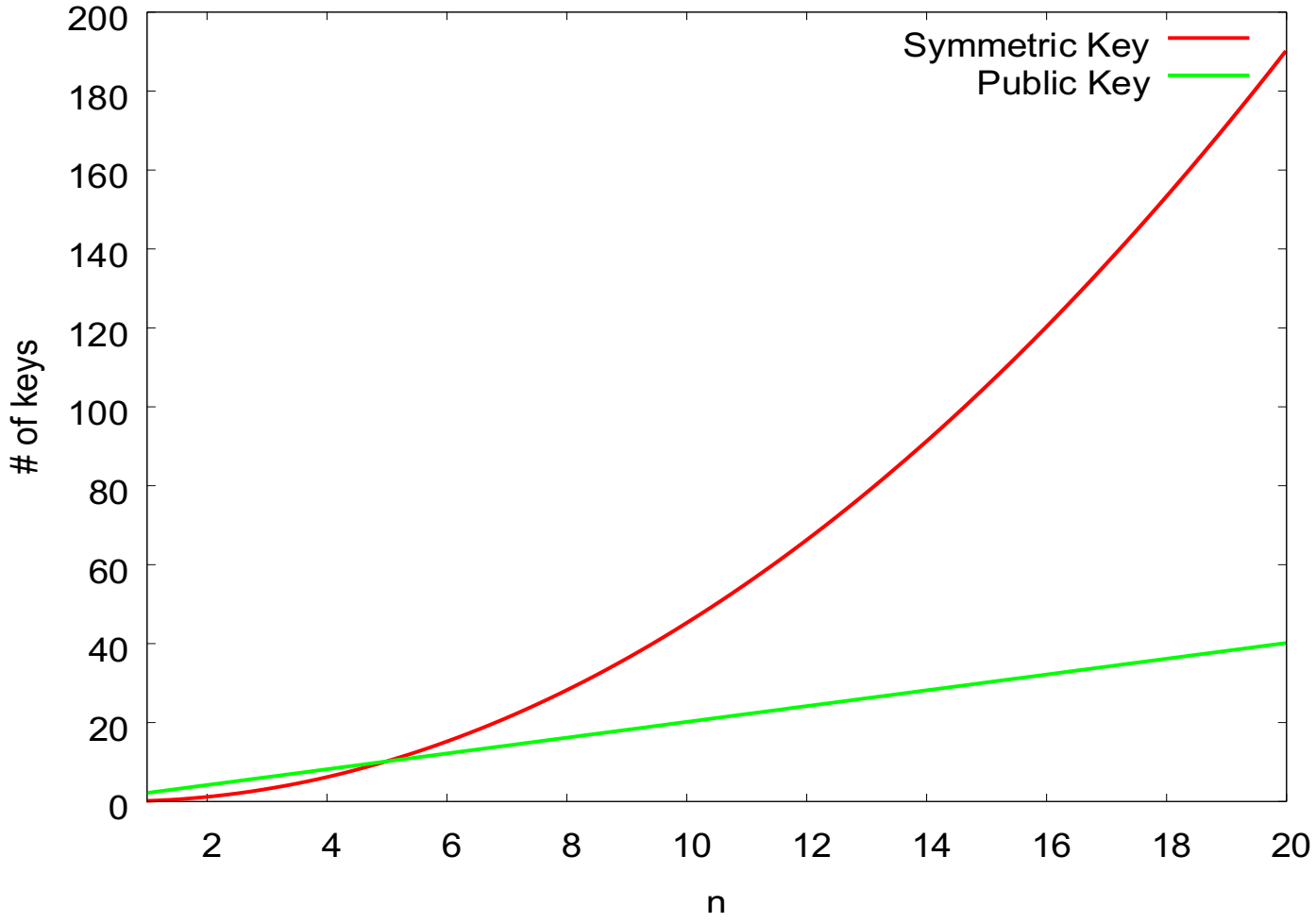
- 公開鍵暗号



$$2n = O(n)$$

n=5の時: 2*5 = 10

総鍵数の増加 (n=ユーザ数)

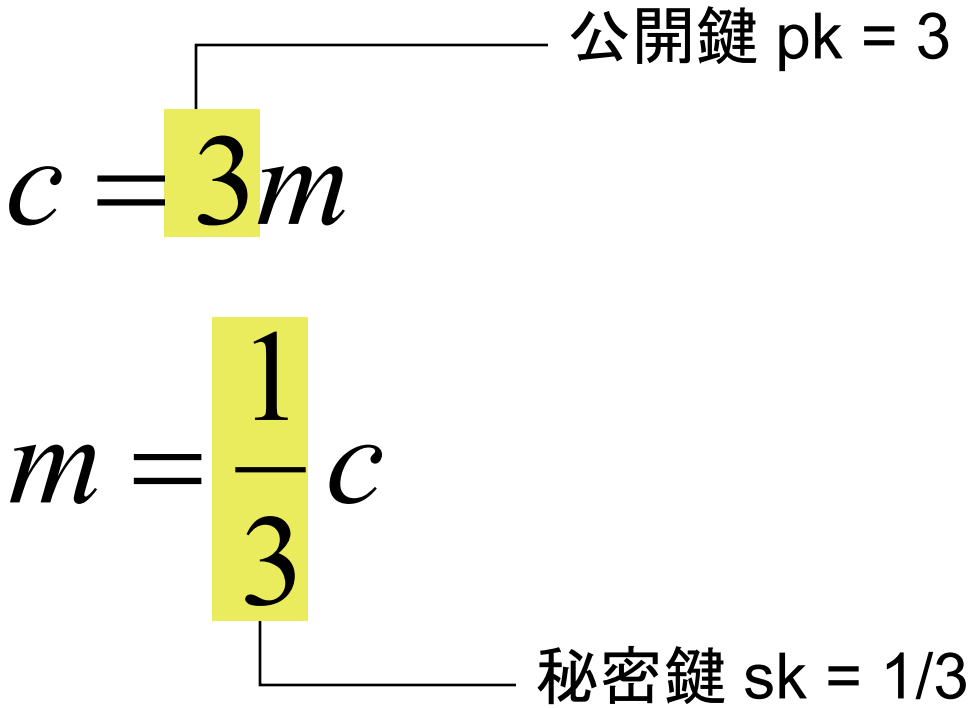


共通鍵暗号と公開鍵暗号

	共通鍵	公開鍵
秘密の共有	事前	不要
送信者の持つ秘密情報	n-1	1
総鍵数	$(n^2-n)/2$	2n
処理速度	高速(Mbps)	低速(kbps)

n=100の時を比べてみよ

公開鍵暗号の原理



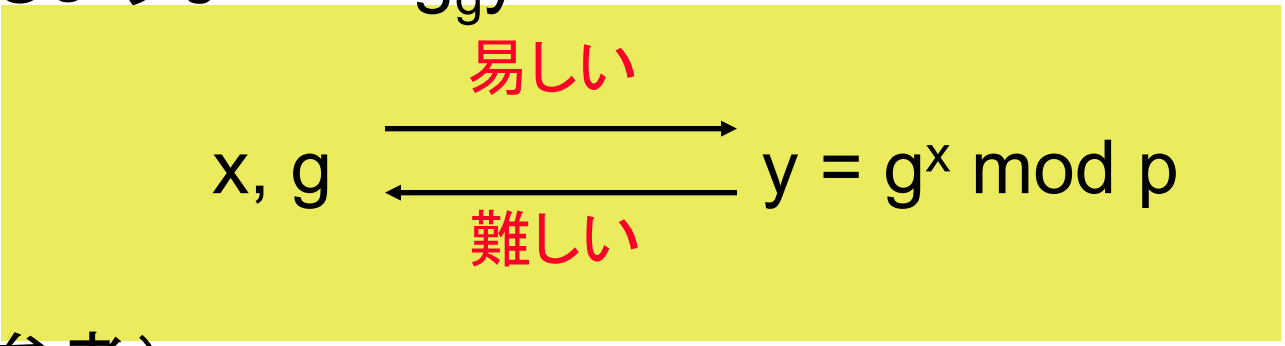
1. pkに対してskは一つ
2. pkからskを求めるのは難しい(?)

公開鍵暗号の種＝「難しい問題」

- 例
  - 割り算
  - 逆行列
  - トラベリングセールスマン問題(TSP)
  - 充足可能性問題(SAT)
  - ナップサック問題
  - 離散対数問題(DLP)
  - 素因数分解問題(IF)

離散対数問題 (DLP)

- 定義
  - yのgに対数離散対数xとは，$y = g^x \bmod p$となるようなx = $\log_g y$.



  - 参考）
    - » 指数計算法　$e^{(\ln n)^{1/3}(\ln\ln n)^{2/3}}$
    - » |p| = 1024 bitが安全とみなされている

公開鍵アルゴリズム

暗号名	発表	提案者	原理	備考
エルガマル	1985	ElGamal	離散対数問題(DLP)	DHに基づく
クレーマ・シュープ(4.3節)	1998	Cramer, Shoup	DLP+安全なHash関数	選択暗号文攻撃に対して安全性証明
楕円(6章)	1985	*	楕円曲線の群でのDLP	鍵長が短く高速
RSA	1977	Rivest, Shamir, Adleman	素因数分解問題(IF)	ディファクト標準 ディジタル署名
ラビン(4.2節)	1979	M. Rabin	IF	安全性の証明
OAEP (4.2節)	1994	Bellare, Rogaway	IF+ランダム関数	PKCS#1 V.2

電子政府推奨暗号

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

平成２５年３月１日
総　　務　　省
経　済　産　業　省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	3-key Triple DES(注3)
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報通信担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

整数論の基礎

乗法群，逆元

菊池暗号

- 鍵生成
  - p: 素数
  - 公開鍵 e (p未満の乱数)
  - 秘密鍵 e•d mod p = 1となるd
- 暗号化
  - c = E(m) = m•e mod p
- 復号
  - d = D(c) = c•d mod p

素数と剰余

- 素数 prime number
  - 約数が自明である(1, a)である整数a
  - 2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 41, 43, 47, 53, …. ∞
  - 合成数: 素数でない数 （負は含まない）
- 剰余
  - a mod n = aをnで割った余り
  - 商　q = [a/n]　a/nを越えない最大の数
  - 剰余（residue）r = a mod n = a - [a/n]n
  - 33 mod 5 = 3
  - 63 mod 11 =　63 – [63/11]11 = 63 – 55 = 8

数値例

- 鍵
  - p = 7, 公開鍵 e = 3, 秘密鍵 d = 5
    (3 • 5 mod 7 = 15 mod 7 = 1)
- 暗号化
  - 暗号化 E(2) = 2 •3 mod 7 = 6
  - 復号　　D(6) = 6 •5 mod 7 = 2
  - E(4) = 4 •3 mod 7 =
  - D(5) = 5 •5 mod 7 =

剰余群1（加法群）

- 加算 $+_6$

  $[a]_n +_n [b]_n = [a + b]_n$

1. $3 +_6 4 = 1$ in Z_6
2. $e = 0$

   $0 +_6 3 = 3 +_6 0 = 3$
3. $1+_6(2+_6 4)= (1+_6 2)+_6 4$
4. $-a = n - a$

   $2 + 4 = 0$

   $-2 = 4$「2の加法の逆元」

   $-4 =$

   $-5 =$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	**0**
2	2	3	4	5	**0**	1
3	3	4	5	**0**	1	2
4	4	5	**0**	1	2	3
5	5	**0**	1	2	3	4

$(Z_6, +_6)$

剰余群2（乗算群）

- $(Z_6, \bullet_6)$
  1. $4 \bullet_6 2 = 2$ in Z_6
  2. e = 1
     $1 \bullet_6 3 = 3 \bullet_6 1 = 3$
  3. $1 \bullet_6 (2 \bullet_6 4) = (1 \bullet_6 2) \bullet_6 4$
  4. $a^{-1} = 1/a$?
     (aの乗法の逆元)
     $5 \bullet_6 5 = 1$
     $5^{-1} =$
     $2^{-1} =$
     $3^{-1} =$

$\bullet_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

乗法群の例

- $(Z_5^*, \bullet_5)$

  $Z_5^* = \{1,2,3,4\}$

  $2^{-1} = 3$

  $3^{-1} = 2$

  $4^{-1} = 4$

- $(Z_7^*, \bullet_7)$

  $4 \bullet_7 2 \equiv 1 \pmod 7$

  $4^{-1} =$

  $2^{-1} =$

$\bullet_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

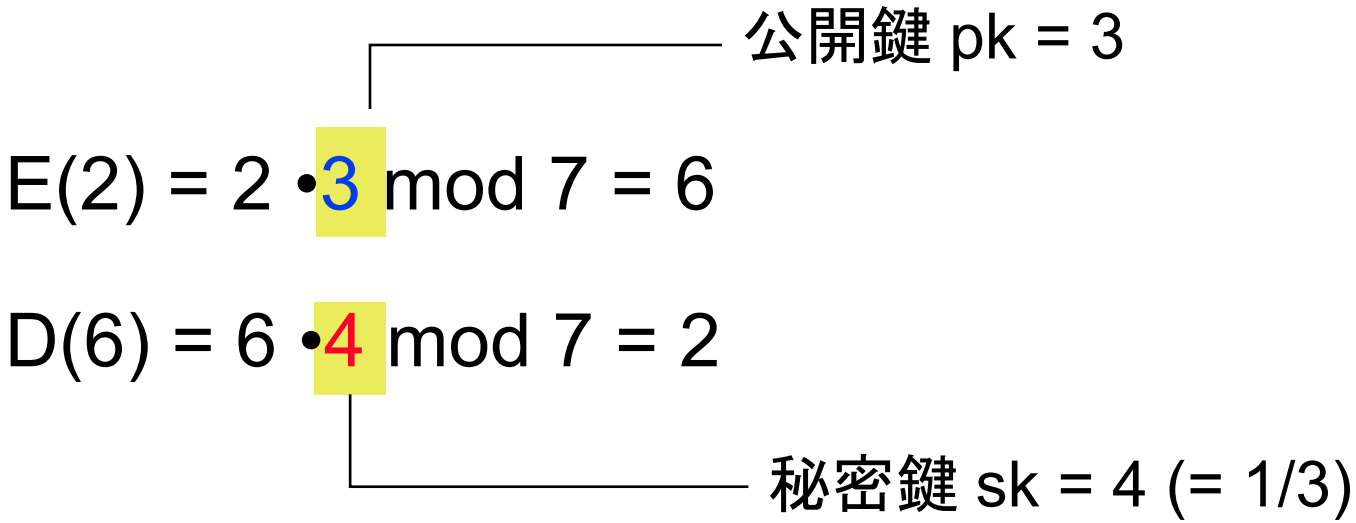
$(Z_5^*, \bullet_5)$

逆元 a^{-1}

- aの（乗法の）逆元 a^{-1}
  - $a \bullet_n b \equiv 1 \pmod n$となるb
  - bの求め方1: n未満の値で総当たり
    - » $3 \bullet 1 \bmod 7 = 3$ no
    - » $3 \bullet 2 \bmod 7 = 6$ no
    - » $3 \bullet 4 \bmod 7 = 1$ yes!
  - bの求め方2: 拡張ユークリッド互除法
- 定理

  $a\,x \equiv b \pmod n$が可解であるための必要十分条件は，$\gcd(a,n) \mid b$.

公開鍵暗号の原理



1. pkに対してskは一つ
2. pkからskを求めるのは難しい(pが大きいとき)

演習

- 次の計算を行え.

1. $8 + 7 \cdot 4 \equiv$ (mod 13)
2. $3 - 7 \equiv$ (mod 13)
3. $6 * 7 * 8 \equiv$ (mod 13)
4. $3^{-1} \equiv$ (mod 13)
5. $4/3 \equiv$ (mod 13)

DH鍵共有

離散対数問題に基づく公開鍵暗号

1. Diffie-Hellman 鍵共有

- W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **22** (1976), 644-654.

http://www-ee.stanford.edu/~hellman/

http://research.sun.com/people/diffie/

2015年チューリング賞

- ACM A. M. Turing Award
  - 計算機科学における ノーベル賞
  - Googleの後援により 100万ドル(1億円)
    - » ノーベル賞は1.2億円
  - 現代計算機科学の父 アラン・チューリング

http://www.nytimes.com/2016/03/02/technology

Alan M. Turing

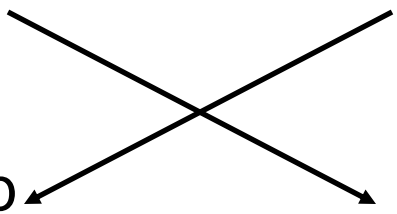
- 業績
  - アルゴリズムの形式術チューリングマシンの提唱，人工知能問題チューリングテスト
  - 第二次大戦英国ブレッチリーパークにて，ドイツ海軍のエニグマ暗号を解読機を開発
  - 同性愛の罪で逮捕．41歳で自殺

D-Hアルゴリズム（鍵共有）

- 準備
  - 素数p, 乗法群 Z_p^*, 原始元 g,

- A
  1. 乱数 $x \in Z_{p-1}$
  2. $a = g^x \bmod p$
  3. $k_A = b^x \bmod p$
     $= g^{yx} \bmod p$
     $= k_B$

- B
  1. 乱数 $y \in Z_{p-1}$
  2. $b = g^y \bmod p$
  3. $k_B = a^y \bmod p$
     $= g^{xy} \bmod p$



2. ElGamal暗号

- 準備
  - 素数p, 乗法群 Z_p^*, 原始元 g,

- B（受信者）
  1. 秘密鍵 $y \in Z_{p-1}$
  2. 公開鍵
     $pk_B = g^y \bmod p$

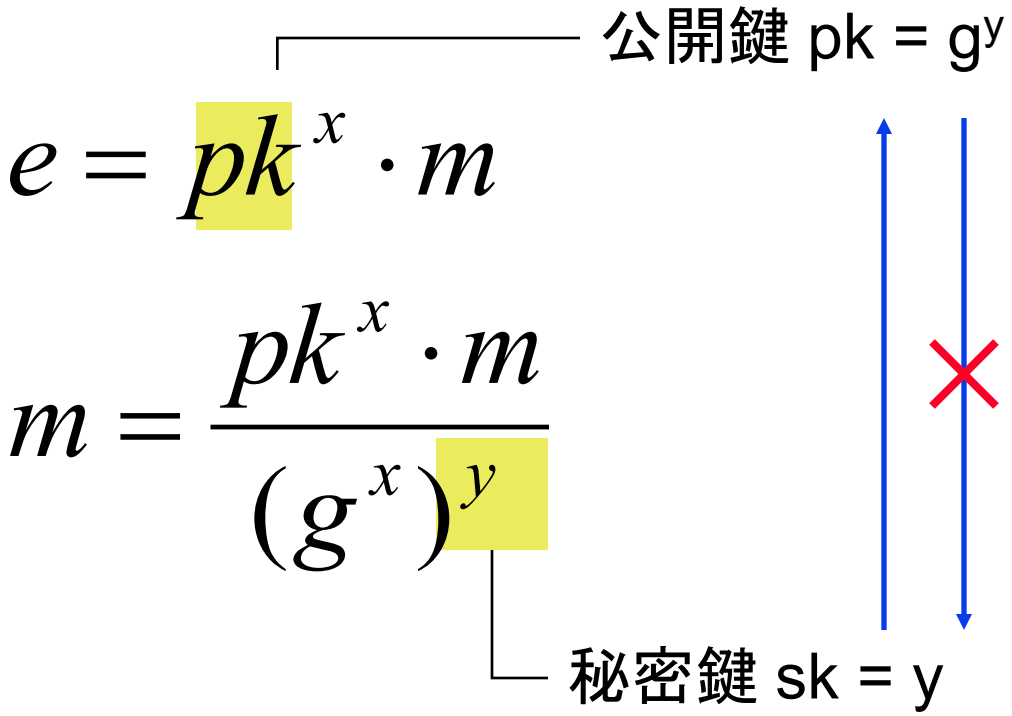
- A(送信者）
  1. 乱数 $x \in Z_{p-1}$
  2. 暗号化 $E_{pk}[m]$:
     $u = g^x$
     $e = m \bullet pk_B^x$
     $(= m\, g^{yx})$

pk_B ←

u,e →

3. 復号
   $m = D_y[u,e]$
   $= e/u^y$
   $= m\, g^{xy} / g^{xy}$

公開鍵暗号の原理



1. pkに対してskは一つ
2. pkからskを求めるのは難しい(Yes!)

演習

- p = 11の情報群Zp*の生成元g = 3 について，DH鍵共有を考える.
- Aは秘密情報x = 3を選び，$a = g^x \bmod p$ をBへ送る．Bも同様に b = 6をAへ送った.
  1. aを求めよ.
  2. Aがbから計算する共有鍵 kを求めよ.
  3. aを盗聴した第三者Cが共有鍵kを求められない理由を述べよ.

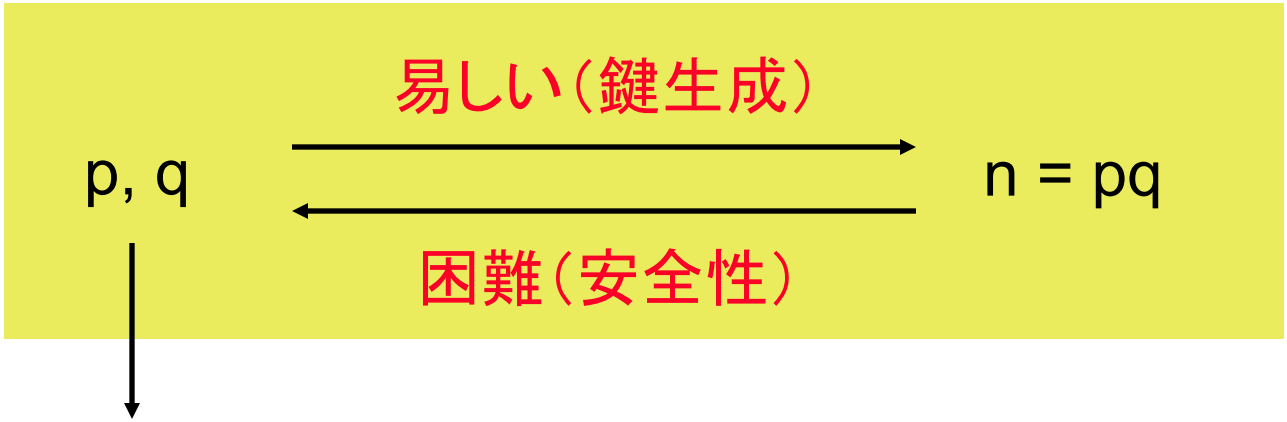
RSA暗号

素因数分解問題に基づく公開鍵暗号

素因数分解問題 (IF)

- 定義

  整数nが与えられたとき，n=pqとなる素因数を求める



RSA暗号

- Rivest, Shamir and Adeleman

  “A method for obtaining digital signatures and publickey cryptosystems”, *Communications of the ACM*, Vol. 21, No.2, pp.120-126, 1978

http://theory.lcs.mit.edu/~rivest/rsa-photo.jpeg

Adi, Ron and Len

RSA小史

- 1976年11月
  - Diffie and Hellman, New Directions in Cryptography, IEEE Trans. on Information Theory, Vol. 22, No. 6, 1976.
- 1976年12月
  - MIT助教授Rivest 29歳, Adelman, Shamirとプロジェクト開始
- 1977年4月3日
  - ユダヤ教祝祭の晩餐（セデル）の夜の閃き
  - MIT LCS TM No. 82, 1977. (4月4日）
- 1977年8月
  - Martin Gardner, A New Kind of Cipher That Would Take Millions of Years to Break, Scientific American, Vol. 237, No. 2, 1977.
  - 100ドル賞金
- 1978年2月
  - CACMにて発表 （公式な誕生）

RSA原著

- Rivest, Shamir, Adeleman

  A method for obtaining digital signatures and publickey cryptosystems, Communications of the ACM, Vol. 21, No.2, pp.120-126, 1978

RSA暗号アルゴリズム

- 鍵生成
  - ランダムな素数 p, q
  - n = pq (合成数）
  - λ(n) = LCM(p-1, q-1)
  - 公開鍵: λ(n)と互いに素なe
  - 秘密鍵: eのλ(n)を法とする乗法逆元
    $d = e^{-1} \bmod \lambda(n)$
    （つまり $ed = 1 \bmod \lambda(n)$）
- 暗号化/復号 （検証/署名）

  暗号化 $C = E(M) = M^e \pmod n$

  復号 $M = D(C) = C^d \pmod n$

数値例

- 鍵生成
  - p = 5, q = 7

    λ(n) =LCM(5-1, 7-1)

    = (4·6)/2 = 12
  - e = 5

    互いに素

    GCD(e, λ(n)) =
  - $d = e^{-1} \bmod \lambda(n)$

    $= 5^{-1} = 5$

    (5·5 mod 12 = 1より)

- 暗号化

  C = E[M]

  $= 4^e \bmod 35$

  = 9

- 復号

  M = D[C]

  $= 9^d \bmod 35$

  $= 9^5 \bmod 35 = 4$

部分群 <a>

- subgroup

  $\langle a \rangle = \{a^k : k \geqq 1\}$

  a: 生成元 generator

  $\langle 2 \rangle = \{2, 4, 1\}$

  $\langle 3 \rangle = \{3, 2, 6, 4, 5, 1\}$

  $= Z_7^*$

  3はZ_7^*の原始元

  $\langle 6 \rangle = \{6, 1\}$

a	a^2	a^3	a^4	a^5	a^6
2	4	1			
3	2	6	4	5	1
4	2	1			
5	4	6	2	3	1
6	1				

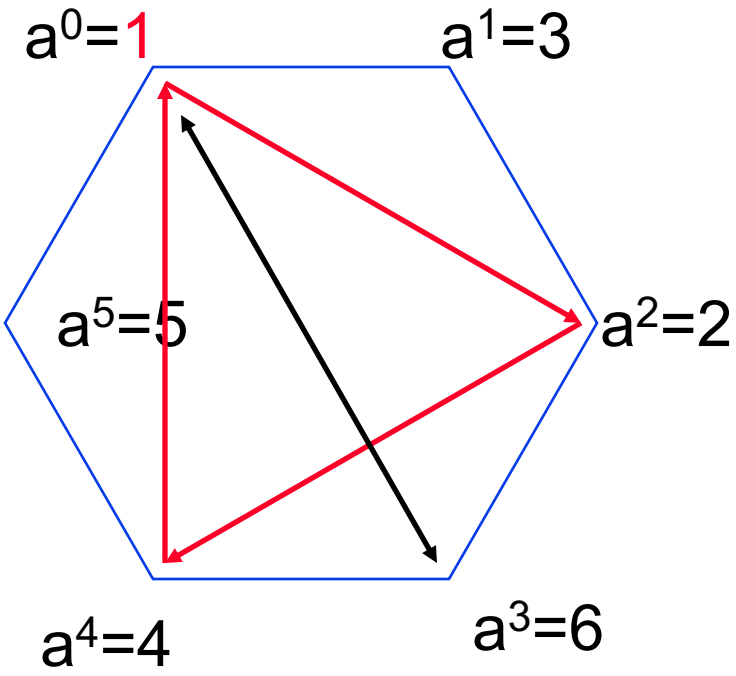
Z_7^*の部分群

位数：$a^t = e$となる最小のt

- 位数 ord(a)
  - $a^t = e$となる最小のt
  - <2> = {2, 4, 1}
  - ord(2) = 3
  - ord(3) =
  - ord(6) =
- 原始元 primitive root
  - ord(a) = $|Z_n^*|$となるa
  - 3, 5はZ_7^*の原始元

a	a^2	a^3	a^4	a^5	a^6
2	4	1			
3	2	6	4	5	1
4	2	1			
5	4	6	2	3	1
6	1				

位数：$a^t = e$となる最小のt



a	a^2	a^3	a^4	a^5	a^6
2	4	1			
3	2	6	4	5	1
4	2	1			
5	4	6	2	3	1
6	1				

Fermat, Pierre de

- 1601-1665
  - Last theorem

    $x^n + y^n = z^n$ を満たす n>2の自然数は存在しない

    “I have discovered a truly remarkable proof which this margin is too small to contain.”

    1995 Andrew J. Wiles
  - Little theorem

http://scienceworld.wolfram.com/biography/Fermat.html

フェルマーの小定理

- 定理 (Fermat)

  素数p, for any a in Z_p^*,

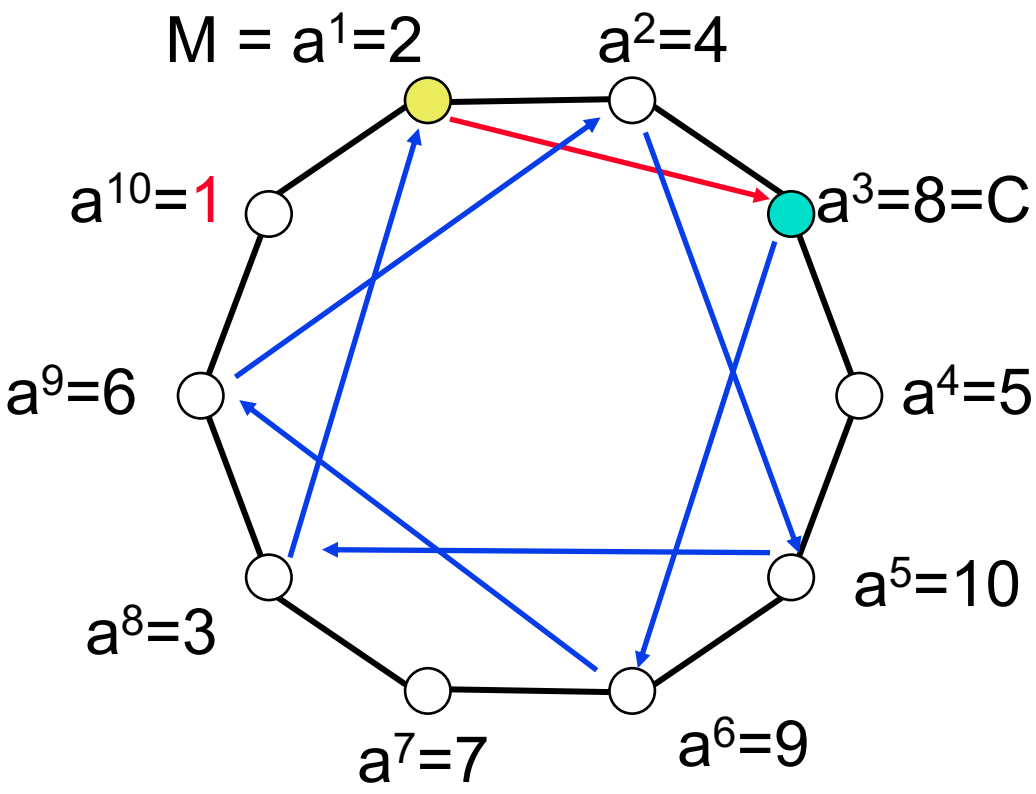
  $$a^{p-1} \equiv 1 \pmod{p}$$

- 例）

1. $8^{10} \bmod 11 = 1$
2. $8^{11} \bmod 11 =$
3. $8^{20} \bmod 11 =$
4. $8^{101} \bmod 11 =$

RSA暗号化と部分群の関係

- Z^*_{11}



- RSA

p = 11

$\lambda(p) = p - 1 = 10$

e = 3

$d = e^{-1} \bmod 10$

$= 7$

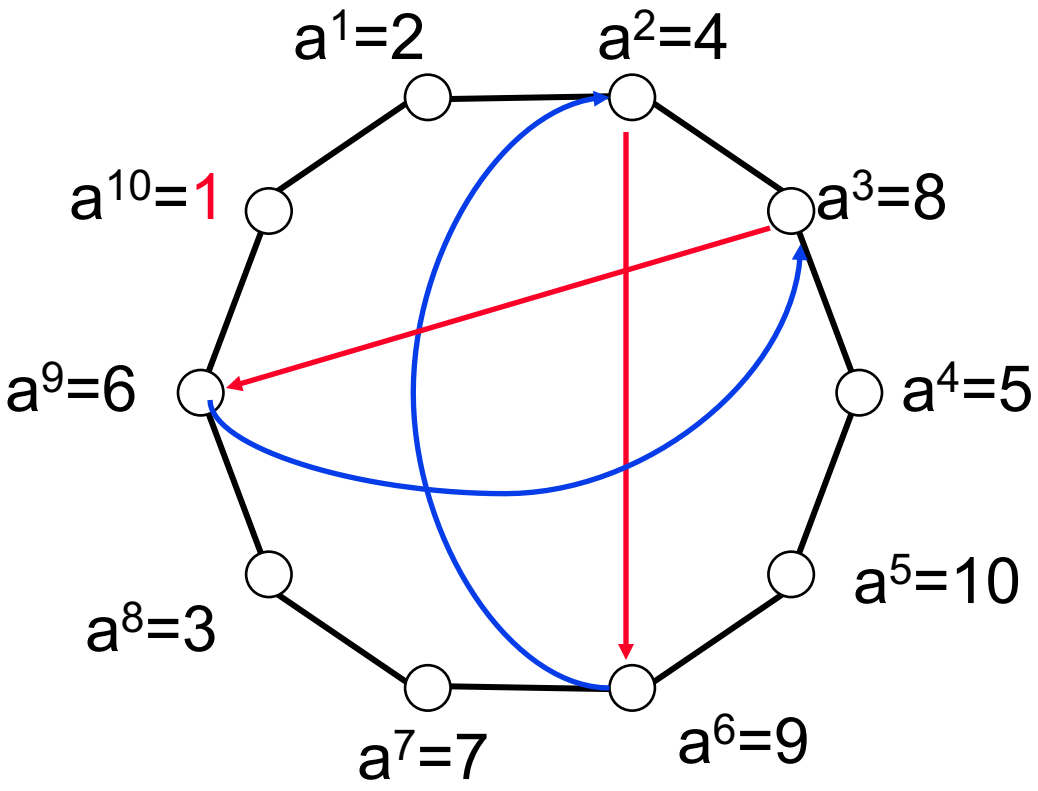
M = 2

$C = M^3 = 8$

$M = C^7 = (a^3)^7 = 2$

RSA暗号化と部分群の関係

- Z^*_{11}



- RSA

p = 11

φ(p) = p –1 = 10

e = 3

d = 7

m = 4

c = E(4) =

m = 8

c = E(8) =

合成数nの時

- RSA暗号

$3^{ed} \equiv 3^{13} \equiv 3 \pmod{35}$

pとqを知っている人にだけ分かる位置

	g	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	g^{11}	g^{12}	g^{13}
p=5	3	4	2	1	3	4	2	1	3	4	2	1	3
q=7	3	2	6	4	5	1	3	2	6	4	5	1	3
n=35	3	9	27	11	33	29	17	16	13	4	12	1	3

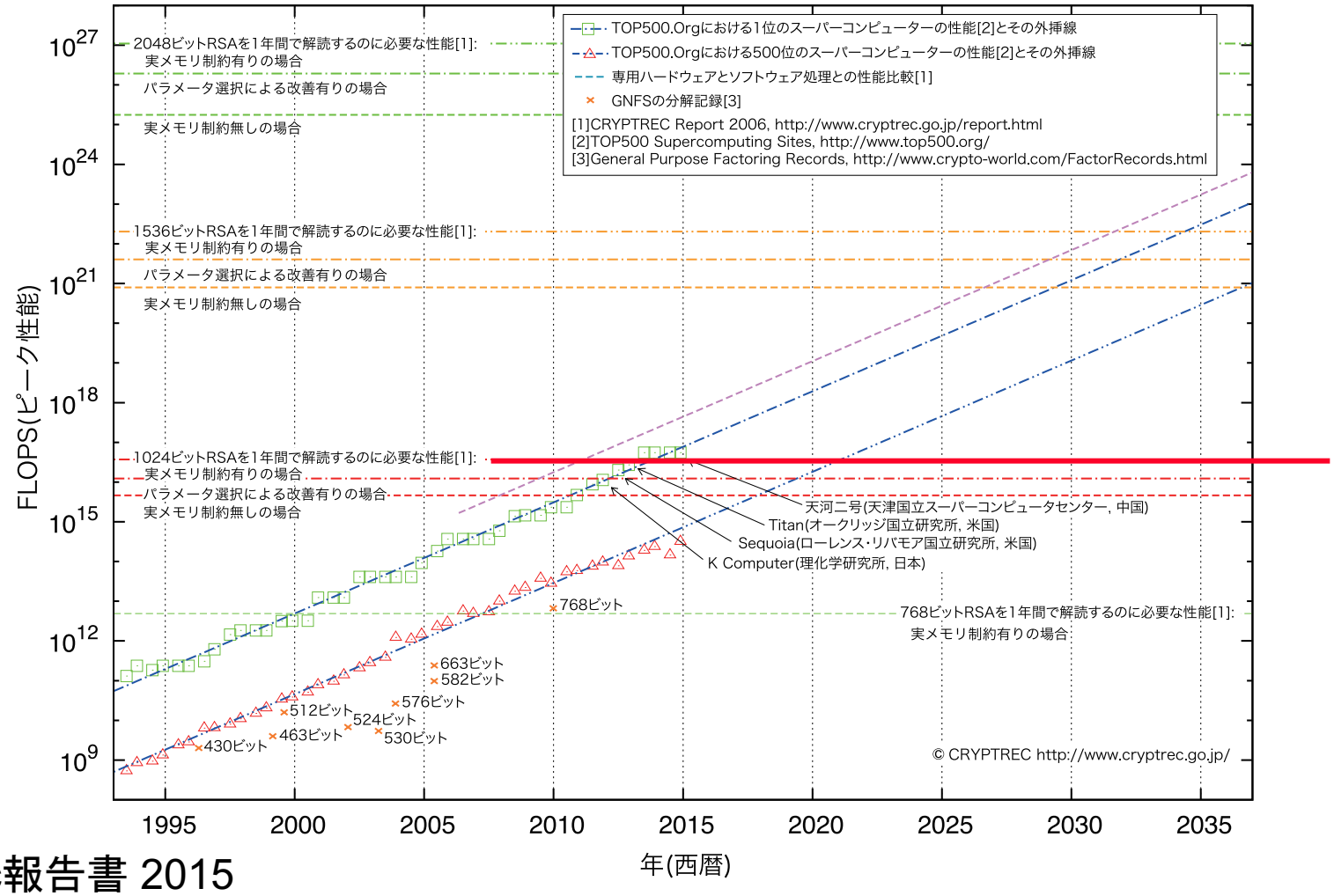
$\lambda(n)=\mathrm{LCM}(p-1, q-1) = \mathrm{LCM}(4,6)=12$

RSA 2010年問題

- 「2010年問題」
  - 2010年に米国NISTの標準暗号アルゴリズムから廃止されるアルゴリズム

	2010年まで（廃止）	2030年まで
共通鍵	2 Key Triple DES	AES, 3 key T-DES
公開鍵	RSA/DSA/DH 1024 bit	同 2048
ハッシュ関数	SHA1	SHA2

RSA暗号を破る処理能力予測



Cryptrec報告書 2015

1 年間でふるい処理を完了するのに要求される処理能力の予測(2015 年2 月更新)

演習

- RSA暗号

  公開鍵n = 5·11 = 55, e = 7のRSAにおいて,

  1. 復号鍵dを求めよ.
  2. 平文 M = 12を暗号化せよ.
  3. 暗号文 c = 8を復号せよ.

まとめ

- 公開鍵暗号では，暗号鍵を(　　)し，復号鍵を(　　)にする．ユーザ数が増えても適用可能な性質を(　　)という．
- DH鍵共有は，(　　)問題の困難性に基づいて設計されている．
- 素因数分解の困難性に基づいて設計されている代表的な暗号に(　　)暗号がある．べき乗を繰り返して最初に単位元1になる値tを(　　)という．