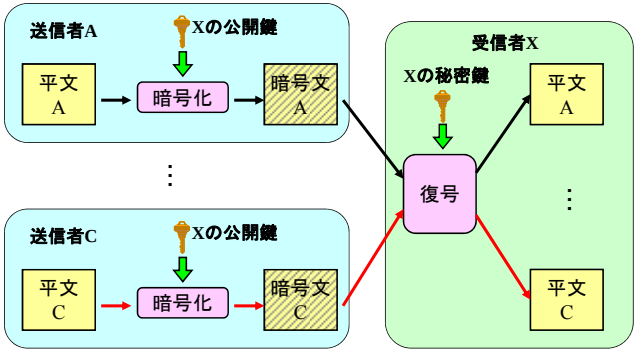
7. 公開鍵暗号

1

公開鍵暗号による暗号化

公開鍵暗号＝非対称鍵暗号

○公開鍵は誰でも使えるので、誰でも暗号文を作れる
○復号できるのは、秘密鍵の所有者のみ



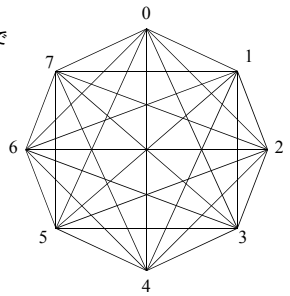
2

共通鍵暗号との違い

共通鍵暗号の場合：鍵の数が増大

・通信する人が8人の場合、全体で
8×(8-1)/2=28個の鍵が必要
（100人の場合は4950個）

・1人当たり7個の鍵を秘密に保持
する必要あり
（100人の場合は99個）

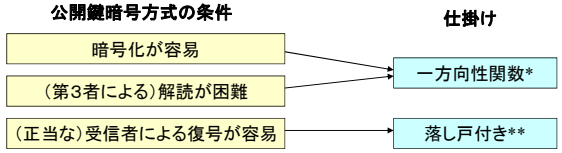


公開鍵暗号の場合：各自の秘密鍵1個と公開鍵1個

・通信する人が8人の場合、必要な鍵は全体で　8×2=16個
（100人の場合は200個）
・秘密に保持するのは各自1個のみ（全体が何人でも同じ）

3

公開鍵暗号の条件と種類



* MからC=f(M)を計算するのは簡単だが、CからM=f^{-1}(C) を計算するのは困難
** 秘密の仕掛けを内部構造に組み込む

利用する数学的性質	方式例
大きい数の素因数分解の困難さ	RSA暗号 Rabin暗号
既約剰余系での離散対数問題の困難さ	Diffie-Hellman鍵配送 ElGamal暗号
楕円曲線上での離散対数問題の困難さ	楕円ElGamal暗号

4

付．公開鍵暗号の例

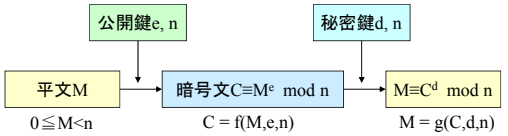
用途	名称	数学問題	開発元	発表年
暗号化	RSA	素因数分解	RSA	1978
	Rabin	素因数分解	Rabin	1979
	ElGamal暗号	離散対数	ElGamal	1982
	EPOC	素因数分解	NTT	1998
署名	RSA	素因数分解	RSA	1978
	ElGamal署名	離散対数	ElGamal	1985
	ESIGN	素因数分解	NTT	1990
	DSA	離散対数	NIST	1991
鍵共有	DH	離散対数	Diffie, Hellman	1976
共通	楕円暗号	楕円曲線上の離散対数	Koblitz, Miller	1985

5

RSA暗号

RSA

・1977年に当時MITにいたRivest（リベスト）、Shamir（シャミア）、Adleman（エールマン）が発明
・代表的な公開鍵暗号方式
・素因数分解の困難さを利用
・平文の値は鍵 n の値より小



6

RSAの仕組み(1)

前提：
・平文を M
・十分大きな2つの素数 p, q を定め、 n = pq とする
・(p−1)(q−1) と互いに素な整数 e を定める ((p−1)(q−1), e) = 1

e と n を公開し（e, n：公開鍵）、p と q を秘密にする

平文Mと暗号文Cの関係

$C \equiv M^e \mod n$

復号はCからMへの逆変換

(p−1)(q−1) とe は互いに素故、以下の逆数dは求まる ← **オイラーの定理** (a, n) = 1 ならば $a^{\varphi(n)} \equiv 1 \mod n$

$ed \equiv 1 \mod (p-1)(q-1)$

7

RSAの仕組み(2)

$ed \equiv 1 \mod (p-1)(q-1)$

$C \equiv M^e \mod n$

$C^d \equiv (M^e)^d \mod n$ ← **合同式の定理**：$a \equiv b \mod n$ ならば $a^k \equiv b^k \mod n$

$ed \equiv 1 \mod (p-1)(q-1)$ 故、$ed = (p-1)(q-1)k + 1$

$(M^e)^d = M^{ed} = M^{(p-1)(q-1)k+1} = M^{(p-1)(q-1)k} M = (M^{(p-1)(q-1)})^k M$

フェルマーの小定理より

$M^{(p-1)} \equiv 1 \mod p$ 両辺をq-1乗すると、$(M^{(p-1)})^{(q-1)} \equiv 1 \mod p$

$M^{(q-1)} \equiv 1 \mod q$ 両辺をp-1乗すると、$(M^{(q-1)})^{(p-1)} \equiv 1 \mod q$

$M^{(p-1)(q-1)} - 1$ がp でもq でも割り切れる。

p、qは素数故、$M^{(p-1)(q-1)} - 1$ がpq、即ちn で割り切れる。

$M^{(p-1)(q-1)} \equiv 1 \mod n$

$C^d \equiv M \mod n$

n = pq、$ed \equiv 1 \mod (p-1)(q-1)$ ならば、$M^{ed} \equiv M \mod n$

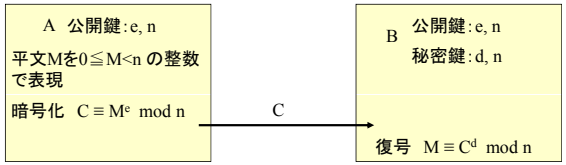
8

RSA方式での暗号化

RSAの公開鍵、秘密鍵

$n = pq$	p, q : 素数
$k = LCM(p-1, q-1)$	LCM : 最小公倍数
$(k, e) = 1$	公開鍵 : e, n
$ed \equiv 1 \mod k$	秘密鍵 : d, n

暗号化



鍵 n(d) として、512, 768, 1024, 2048ビットが使用されている
（1024ビット以上が望ましい）

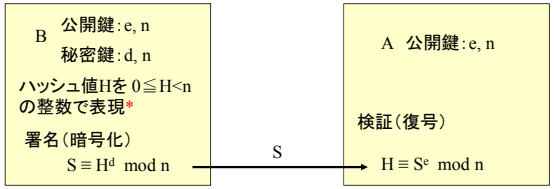
9

RSA方式でのディジタル署名

RSAの公開鍵、秘密鍵

$n = pq$	p, q : 素数
$k = LCM(p-1, q-1)$	LCM : 最小公倍数
$(k, e) = 1$	公開鍵 : e, n
$ed \equiv 1 \mod k$	秘密鍵 : d, n

署名



$ed \equiv 1 \mod k$ より、e とd は逆数。署名は暗号化の逆操作で可能

* 署名対象のサイズが n–1で抑えられることが文書のハッシュを取る理由の1つ

10

付. RSA公開鍵、秘密鍵の例

公開鍵 e (17 ビット) 65537 (0x10001)

n (1024 ビット) d2:de:6d:97:b1:9f:a3:62:ec:c7:e5:f8:97:3d:
cd:01:00:26:e7:59:49:05:68:9d:0a:62:3a:a7:ea:
5d:54:b7:1c:be:12:91:41:58:53:2e:b8:5a:9a:d6:
0c:48:52:3a:71:8f:0c:56:97:b7:10:f4:d7:98:aa:
30:b7:59:c6:06:4f:04:f0:f2:07:fe:6b:b4:b4:f5:
f5:91:a0:56:5e:cb:b0:23:58:58:85:d4:da:d9:85:
76:96:88:8d:00:fd:40:53:c5:f2:4b:a8:00:9c:fb:
ed:3e:a0:9a:c5:d4:9e:1e:fc:ea:83:1b:96:33:62:
5f:41:67:ce:5c:f3:12:0a:53

秘密鍵 d (1024 ビット) 46:57:98:ab:6f:bf:57:1b:9a:ed:1c:14:0f:2f:b8:
81:4a:f1:af:5f:23:72:c0:71:12:93:ae:09:71:ae:
ec:a1:a0:de:ef:06:b1:8b:ab:43:fc:8f:8c:f3:36:
69:b1:b4:79:49:44:ce:66:11:d5:80:37:a3:5f:b2:
9c:97:3f:ed:23:bb:fb:09:19:bc:5a:6a:bc:14:e0:
39:dc:77:4a:b2:8d:a6:6b:67:ab:ac:f2:50:47:41:
62:30:ad:24:a5:05:4a:56:50:b3:9e:80:e2:32:d9:
b7:ec:55:13:11:21:02:b0:f2:c4:29:3e:f0:04:64:
6a:a1:ce:8f:53:6e:64:41

11

RSAでの鍵の計算例

相異なる素数を p=2, q=17 とする

$n = pq = 2 \times 17 = 34$

$k = LCM(p-1, q-1) = LCM(2-1, 17-1) = LCM(1, 16) = 16$

$(k, e) = 1$ より、e=3 とする

公開鍵は n=34, e=3 となる

$ed \equiv 1 \mod k$ より $3d \equiv 1 \mod 16$ (1)

恒等的に成り立つ式 $16d \equiv 0 \mod 16$ (2)

16と3にユークリッドの互除法を適用 $16 = 5 \cdot 3 + 1$
$3 = 3 \cdot 1$

×5 が必要

(1)×5 $15d \equiv 5 \mod 16$ (3)

(2) – (3) $d \equiv -5 \mod 16$

$d \equiv 11 \mod 16$

秘密鍵 d =11

12

RSAでの暗号化復号例

公開鍵 e=3、n=34

0≦M<n を満たす平文M=26 の暗号化

$C \equiv M^e \mod n = 26^3 \mod 34$

$26^3 \equiv (-8)^3 = (-8)^2(-8) \equiv (-4)(-8) = 32 \mod 34$

暗号文C=32

秘密鍵 d =11、n=34

復号

$M \equiv C^d \mod n = 32^{11} \mod 34$

$32^{11} \equiv (-2)^{11} = ((-2)^5)^2 (-2) \equiv 2^2(-2) = -8 \equiv 26 \mod 34$

平文M=26

13

素因数分解の困難さの利用

送信者：平文Mに対する暗号文Cを作成

$C \equiv M^e \mod n$　　公開鍵：e, n

一方向性　・MからCを計算するのは容易（**送信者**）
・CからMを計算するのは困難（**解読者**）

受信者：暗号文Cから平文Mを復号

$M \equiv C^d \mod n$　　秘密鍵：d

CからMを計算するのは容易（**受信者**）

↑

dが既知

↑

eからd を計算できる（落し戸）　$ed \equiv 1 \mod LCM(p-1, q-1)$

↑

LCM (p–1, q–1)を計算できる

↑

p, qが既知　n = pq

受信者以外：nからp, qを計算するのは困難（素因数分解の困難さ）

14

RSAの利用

RSA暗号は計算時間がかかるので、通常は鍵配送時の鍵の暗号化に使用

平文が短い場合、大きな乱数を連結する

公開鍵のeの値

・e は固定値でもよい（安全性は低下しない）
・e が小さいと、使用頻度の高い暗号化と署名検証の処理が早くなる
・e として、3 と 65537（$2^{16}+1$）がよく使われる

公開鍵のn は秘密鍵対応に異なる値

15