RSA 暗号について　　加本

＜１＞ RSA における「公開鍵」と「秘密鍵」の関係

1. まず前提

RSA では、メッセージのやり取りを安全にするために、

暗号化には公開鍵を使う　復号には秘密鍵を使う　という「役割分担」があります。

ただし、この 2 つの鍵は全くの別物ではなく、数学的に対になっています。

2. 例で考える（概念）

たとえば、ある人（B さん）が RSA 鍵を作ると、次のような鍵のペアができます：

公開鍵（B の）　例：（n = 3233, e = 17）　→ この「公開鍵」は誰でも使ってよい（ネットに公開しても OK）

秘密鍵（B の）　例：（n = 3233, d = 2753）　→ この「秘密鍵」は B さんだけが知っている（絶対に他人には見せない）

※ここで n は 2 つの素数の積、e は公開用指数、d は秘密の指数です。これらの具体的な計算は省略します。

3. 公開鍵と秘密鍵の関係性のポイント

公開鍵（n, e）で暗号化したものは、秘密鍵（n, d）でしか復号できません。

秘密鍵（n, d）で署名したものは、公開鍵（n, e）で検証できます。

つまり：公開鍵と秘密鍵は「逆向きに作用する、ぴったり対応したペア」なのです。

4. 通信の流れ（暗号化の例）

登場人物：A さん（送り手)、B さん（受け手）

手順：

B さんは、自分用の RSA 公開鍵と秘密鍵のペアを作る。

B さんは、公開鍵だけを A さんに送る。

A さんは、その公開鍵を使ってメッセージを暗号化する。

A さんは、暗号化されたメッセージを B さんに送る。

B さんは、自分の秘密鍵を使ってメッセージを復号する。

➡ この仕組みのおかげで、第三者は内容を読めません。

◆ なぜ安全なのか？

公開鍵から秘密鍵を「逆算」するのは非常に困難（現在の計算機では数千年かかる)。

公開鍵を使って暗号化しても、秘密鍵なしには元に戻せない。

＜２＞　RSA 暗号の具体例：公開鍵・秘密鍵による暗号化と復号

1. 鍵の設定

以下は RSA の簡易な例です。

公開鍵（誰でも使ってよい）: (n = 3233, e = 17)

秘密鍵（本人だけが知る）: (n = 3233, d = 2753)

2. 平文の設定

ここでは、文字 'A' の ASCII コードである 65 を平文として使います。

3. 暗号化

平文 65 を公開鍵（n = 3233, e = 17）を使って暗号化します。

計算式: 暗号文 = 65^17 mod 3233

結果: 暗号文 = 2790

4. 復号

暗号文 2790 を秘密鍵（n = 3233, d = 2753）を使って復号します。

計算式: 復号結果 = 2790^2753 mod 3233

結果: 復号結果 = 65（元の 'A' に戻る）

5. まとめ

このように、RSA では公開鍵で暗号化したメッセージは対応する秘密鍵でしか復号できません。逆に、秘密鍵で署名したものは公開鍵で検証できます。このような性質により、安全な通信や電子署名が実現されています。

＜３＞　RSA 暗号における鍵と安全性の関係：例（n=3233, e=17, d=2753）

1. はじめに

RSA 暗号は、大きな数を素因数分解することが困難であるという性質に基づいています。公開鍵（n, e）と秘密鍵（n, d）は数学的に対応しており、一方で暗号化したものは、他方でしか復号できません。

2. この例の鍵情報

公開鍵: (n = 3233, e = 17)

秘密鍵: (n = 3233, d = 2753)

3. n の正体：素因数分解

n = 3233 は以下の素数の積でできています：

p = 61, q = 53

したがって、n = p × q = 61 × 53 = 3233

4. ϕ(n) の計算と鍵の関係

RSA では次にオイラー関数 ϕ(n) を計算します。

ϕ(n) = (p - 1)(q - 1) = 60 × 52 = 3120

この ϕ(n) に対して、e = 17 は互いに素な数として選ばれました。

次に、以下を満たす d を求めます：

d × e ≡ 1 mod ϕ(n) → d × 17 ≡ 1 mod 3120

この条件を満たす d = 2753 です。

5. なぜ安全なのか

このように、n の素因数（p, q）を知らない限り ϕ(n) を計算することは困難です。したがって、秘密鍵 d を導くのは非常に難しいという点が RSA の安全性の根本にあります。

6. まとめ

・公開鍵と秘密鍵は、n を共有しつつ異なる指数（e, d）を持つ。

・n は 2 つの素数の積として成り立ち、その分解が困難なため、第三者が秘密鍵を割り出すのは困難。

・今回の例では、17 と 2753 は n を構成する素数とは関係がなくても、鍵として機能します。

・ただし、これらの値は ϕ(n) との関係で正しく構築されたペアでなければなりません。