速習RSA

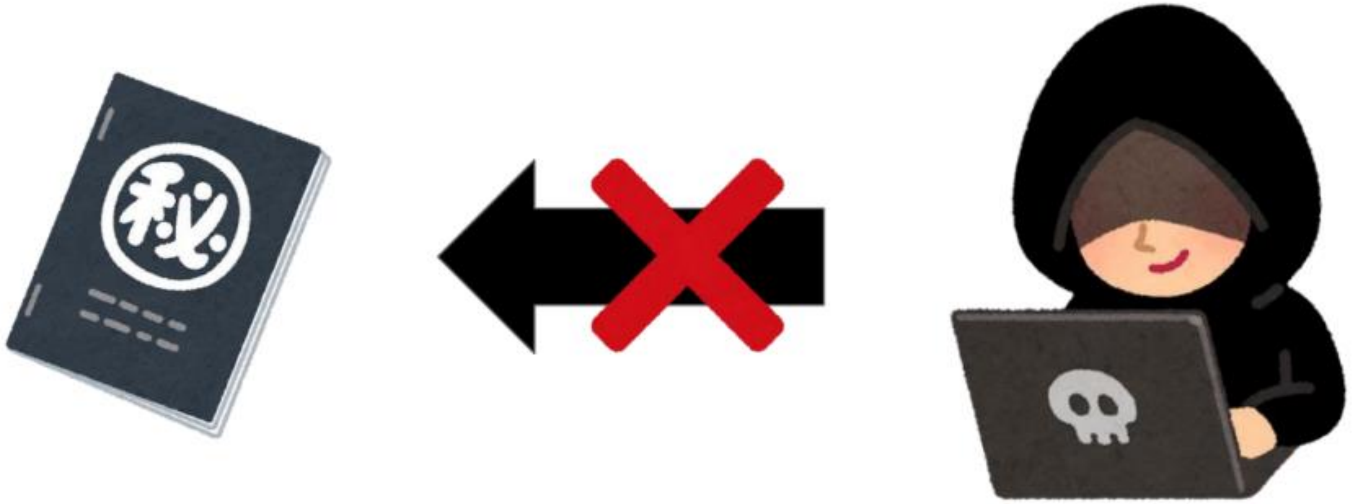
曖昧な理解からの脱却

暗号の必要性

例）ネットショッピング

カード情報がそのまま送信されると外部に筒抜け

→ 悪用されるリスク



基本用語

- 平文 … 元の文章のこと
- 暗号文 … 平文に操作を施して意味を読み取れなくした文章

- 暗号化 … 平文から暗号文を得ること
- 復号 … 暗号文から平文を得ること

- 鍵 … 暗号化と復号に必要なもの

遥か昔

- シーザー暗号

アルファベットをずらす暗号化方式
ずらす文字数をnとすれば、nが鍵といえる
例）「hello」→「khoor」（3文字ずらし）

- スキュタレー暗号

文字がびっしり書かれた細い紙を筒に巻き付ける暗号化方式
平文のうちの1文字が一定間隔で配置される

共通鍵暗号方式（1/2）

先ほど見てきた暗号は、次のような特徴がある

- シーザー暗号

何文字ずらすかを事前に共有する必要がある

- スキュタレー暗号

両者で同じ筒を用意する必要がある

つまり、暗号化・復号に同じもの（鍵）を用いる
→ 共通鍵暗号方式

共通鍵暗号方式（2/2）

他にも
- バーナム暗号
- DES
- AES（DESの進化版）

など、様々な共通鍵暗号が存在する
しかし、鍵を共有する時点で漏洩したらすべてが破綻してしまう

この弱点を解消できないか？ → 公開鍵暗号方式

公開鍵暗号方式（1/3）

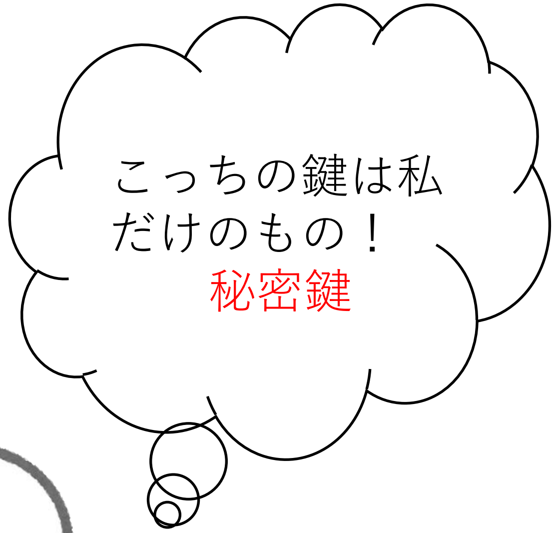
公開鍵暗号とは
暗号化するための鍵と復号するための鍵が異なる暗号

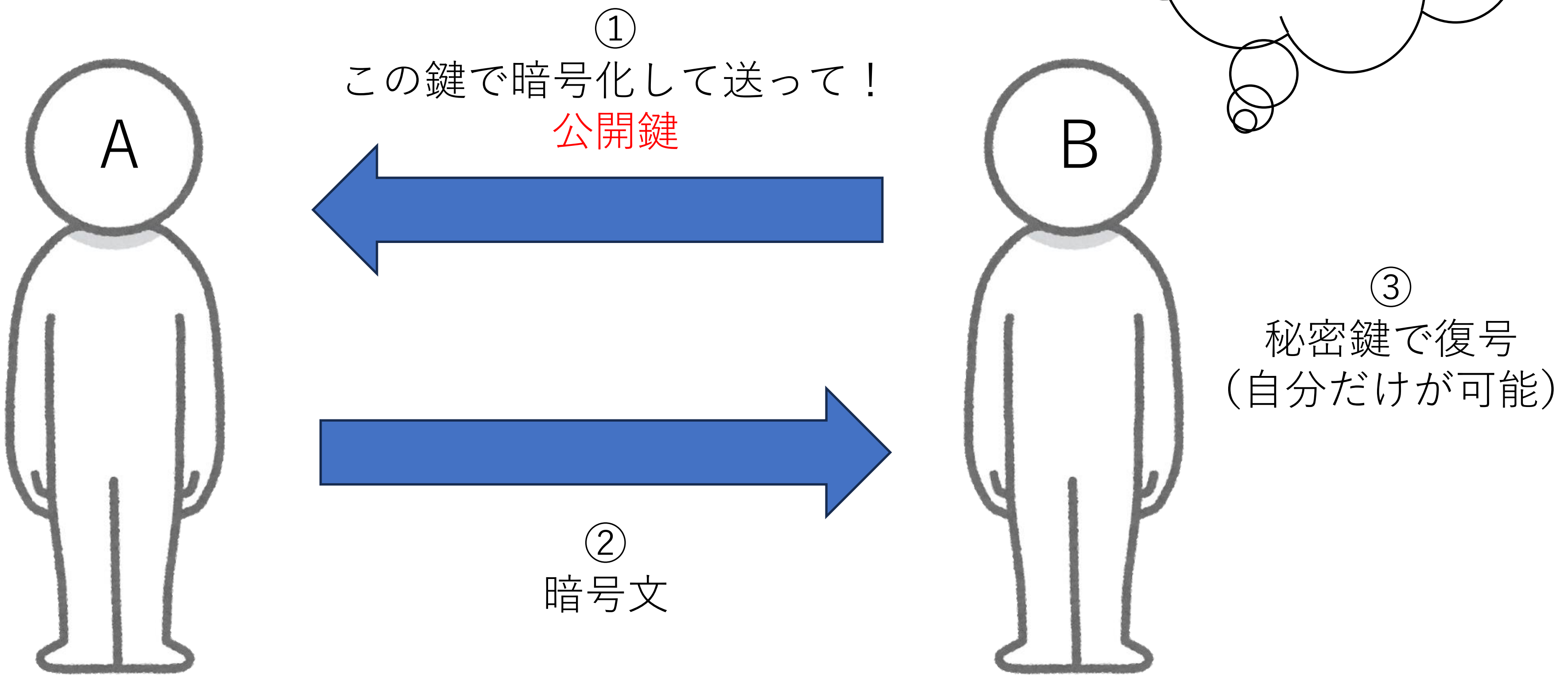
以降、次のような状況を想定する

Aさん（送信者）　→　Bさん（受信者）

次のスライドにて流れを図示する

公開鍵暗号方式（2/3）


こっちの鍵は私
だけのもの！
秘密鍵


①
この鍵で暗号化して送って！
公開鍵
A
B
③
秘密鍵で復号
（自分だけが可能）
②
暗号文

公開鍵暗号方式（3/3）

ツッコミ
「なんとなく言いたいことはわかるけど、
　鍵がどうのこうの言われてもいまいちピンと来ない」

RSA暗号（後述）が公開鍵暗号方式の１つというのは聞いたことがある人は多いと思われる

RSA暗号にまつわる、よくある説明として「素因数分解の困難性」といったものがあるが、処理の流れと組み合わせなければピンとこないのが実情である

RSA暗号（1/8）

「根本的な発想」

$$a^{ed} \equiv a \ (mod \ n)$$

ただし、aは平文、$n = pq$（p, qは異なる素数）

上記が実現できるようなe, dを適切に選ぶことができれば、

暗号化 : m^eをnで割った余りを取り、暗号文cを取得

復号 : c^dをnで割った余りを取って復号し、mを取得

といった具合にうまく元に戻る

ではどう実現するか？ → オイラーの定理（別紙）を利用する

RSA暗号（2/8）

つまり、
暗号化に必要なモノ：n, e
復号に必要なモノ：d（nは既知より、dのみでよい）

言い換えれば、
Bさんの公開鍵：(n, e)　※ n, eの順序付きの組（区別するため）
Bさんの秘密鍵：d

RSA暗号（3/8）

「体験」

$p = 3, q = 5$として、互いに異なる素数をとる

このとき、$n = pq = 3 \times 5 = 15$

よって、暗号化及び復号の際は$mod 15$の世界で考える

$(p-1)(q-1) = 2 \times 4 = 8$と互いに素な整数として$e = 7$をとる

公開鍵の構成要素の1つeに応じた秘密鍵として、$d = 7$をとる

ここで、平文を$a = 2$とする

暗号化：$c = a^e \, mod \, 15 = \; 2^7 mod \, 15 = 8$ ← 暗号文

復号：$a = c^d \, mod \, 15 = \; 8^7 \, mod \, 15 = 2$← 元に戻った

RSA暗号（4/8）

オイラーの定理（別紙）より、

$$a^{k(p-1)(q-1)+1} \equiv a \ (mod\ n)$$

つまり、$ed = k(p-1)(q-1)$ となるようにeとdを決定すると、
RSA暗号はうまく機能することがわかる

RSA暗号（5/8）

eは、$(p-1)(q-1)$と互いに素になるように適当にとればよい

そうなると、どのようにdをとれば適切だろうか？

$$ed = k(p-1)(q-1) + 1$$

の形になればよいことを思い出すと、

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

を満たすdをとればよいことがわかる

なぜならば、edを$(p-1)(q-1)$で割った余りが1であるということは、ある整数kが存在して、$ed = k(p-1)(q-1) + 1$ となることに他ならないからである

RSA暗号（6/8）

前述した通り、

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

となるようなdがほしい

どうdを決定するか？ → 「拡張ユークリッド互除法」（別紙）

RSA暗号（7/8）

eと$(p-1)(q-1)$は互いに素としたため、最大公約数は1

すなわち、拡張ユークリッド互除法より、

$$ex+(p-1)(q-1)y=1 \cdots ①$$

を満たす整数の組(x,y)が存在する

このとき、$x\ mod\ (p-1)(q-1)$の結果 $\cdots$ ② をdとすればよい

なぜならば、①を式変形して

$$ex=-(p-1)(q-1)y+1$$

より、$ex\equiv 1\ (mod\ (p-1)(q-1))$であるから、

$(p-1)(q-1)$を法として合同な②をdとしてよいからである

RSA暗号（8/8）

eは適当にとり、dを適切に決定できたとする

これにより、(n, e)を公開して送信者であるAさんに暗号化してもらい、受け取った暗号文を、受信者であるBさんだけが知っているdにより復号するという仕組みが成り立つ状況が完成し、安全な通信が実現できる

攻撃者の視点（1/2）

素因数分解の困難性はどこで威力を発揮するか？

RSA暗号は、公開鍵(n, e)から誰でも暗号化して送信することができる

つまり、攻撃者にとってnとeは既知であり、そこからdを割り出すことができれば復号可能となり、通信を筒抜けにできる

前述の通り、

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

となるようなdは拡張ユークリッド互除法により計算可能だが、

法を$(p-1)(q-1)$で考えている以上、２つの素数p, qがわからないとdを求められない

攻撃者の視点（2/2）

攻撃者にとって既知である$\boldsymbol{n}$から$\boldsymbol{p}$と$\boldsymbol{q}$を求める作業が必要

これは、要するに$\boldsymbol{n}$を素因数分解することである

2つの素数$\boldsymbol{p}, \boldsymbol{q}$を十分大きくとれば$\boldsymbol{n}$の桁は大きい

→ $\boldsymbol{n}$の素因数分解は困難

→ 解読に時間がかかる

→ 解読できたころには、その情報は無価値（つまり安全）

問題

$p = 3, q = 5$のRSA暗号を既に体験してもらった
今まで学習した内容を総動員して数学的に捉えなおしましょう

1. $(n, e) = (15, 7)$は公開鍵となることを示せ
2. 公開鍵(n, e)に対応する秘密鍵dを決定せよ
3. 平文が$a = 3$であるとき、暗号文cを求めよ
4. 上で求めた暗号文cを復号し、平文と一致することを確認せよ

解答（1/4）

1.

eが、$(p-1)(q-1)$と互いに素であればよい

$e=7, (p-1)(q-1)=8$より、互いに素

よって、与えられた(n, e)は公開鍵となる

解答（2/4）

2.

dを具体的に決定するために、拡張ユークリッド互除法を用いる

$n_0 = (p-1)(q-1) = 8, n_1 = e = 7$とすると

i	n_i	q_i	x_i	y_i
0	8		1	0
1	7	1	0	1
2	1	7	$x_0 - q_1 x_1 = 1$	$y_0 - q_1 y_1 = -1$
3	0			

解答（3/4）

よって、$i=2$の行に着目すると

$$1 = (p-1)(q-1) \times 1 + e \times (-1)$$

を得る

式変形すると

$$e \times (-1) = -(p-1)(q-1) + 1$$

となるが、$(p-1)(q-1)$で割る操作を考えると

$$e \times (-1) \equiv 1 \ (mod \ (p-1)(q-1))$$

なので、$-1 \equiv 7 \ (mod \ (p-1)(q-1))$ より、

$$d = 7$$

解答（4/4）

3.

暗号化すると

$$c = a^e \, mod \, n = \; 3^7 \, mod \, 15 = 12$$

4.

復号すると

$$c^d \, mod \, n = \; 12^7 \, mod \, 15 = 3$$

これは平文に一致

ハイブリッド暗号方式

公開鍵暗号（RSA暗号など）
→ 大きな整数のべき乗剰余の計算が必要なので処理時間が長い

共通鍵暗号（AESなど）
→ 鍵が漏洩したら一巻の終わりだが、処理時間が短く高速

共通鍵暗号の鍵を、公開鍵暗号で配送し、
以降は共通鍵暗号による通信をすれば安全かつ高速

デジタル署名（1/4)

想定する状況 : RSAによる共通鍵の交換

→ 問題点 : 交換する相手が本物なのか？
なりすましているのではないか？

この問題の解決策：「デジタル署名」

秘密鍵は本人だけが知っているという性質を利用したもの

RSA暗号による暗号化の逆をやるイメージ

デジタル署名（2/4）

①自分 : ある文書Mを送る

②相手 : Mを受けとり、それをハッシュ化してmにする

③相手 : $(M, m^d\ mod\ n)$を送信

④自分 : Mをハッシュ化したものと、
$m^{de}\ mod\ n$ が一致するかどうか確認する

→ ④にて、一致すれば相手は本人であると判断する

ただし、e, dはそれぞれ、相手の公開鍵と秘密鍵である

デジタル署名（3/4）

なぜそれで判定できるのか？

→ ハッシュ関数は、同じ値を入力すれば同じ出力が返ってくる

また、秘密鍵は本人しか知らない

更に、公開鍵で正しく復号できればそれらがペアとわかる

→ 通信相手は本人である

※ ハッシュ関数は、

①復元困難、②同じ入力なら同じ出力　という特徴がある

デジタル署名（4/4）

更に、
- 公開鍵の発行元情報
- 署名アルゴリズム（RSAなど）
- 署名ハッシュアルゴリズム（MD5など）
- 有効期間
- 認証局のデジタル署名

などが記された「公開鍵証明書」を、認証局（信頼性のある第三者機関）が発行することにより、相手の公開鍵の正当性が担保されている

→ この一連の流れが、HTTPSの「S」が示す、
暗号化通信プロトコル「SSL/TLS」を形作る