

2022 年度 山梨大学工学部 オープンキャンパス
コンピュータ理工学科 模擬授業

秘密情報を守ろう
～暗号技術入門～



担当教員：盧 晓南
ロ ギョウナン

2022 年 8 月 6 日

暗号とは？

- 以下の中に「暗号」およびその応用に当てはまるものは？



(a) 合言葉



(b) 暗証番号



(c) マルウェア



(d) IC カード

- 狭義の暗号技術：情報を送り手、受け手以外には読めなくする方法
- 広義の暗号技術：秘密情報の漏洩（盗聴）・改ざん（不正な書き換え）から守る技術

古代ローマ時代の暗号：シーザー暗号

ガイウス・ユリウス・カエサル

- Gaius Iulius Caesar (100BC – 44BC, 共和政ローマ末期の政治家, 軍人, 文筆家. 古代ローマで最大の野心家と言われる) が使用した
- Caesar の英語読み「シーザー」で「シーザー暗号」と呼ばれている

シーザー暗号における暗号文の作成手順

通常のアルファベットを右(または左)に何文字かずらす

通常のアルファベット	A	B	C	D	…	W	X	Y	Z
暗号化アルファベット	D	E	F	G	…	Z	A	B	C

演習1：シーザー暗号を解読してみよう！

以下のウェブページにアクセスしてください

<http://www.kki.yamanashi.ac.jp/~xnlu/oc2022/>

- 暗号文が表示される
- 解読 (左に1文字ずらす) を押すと、暗号文を左に1文字ずらした文字列が表示される
- 平文 (意味を持つ文字列) が出るまで繰り返して押していく

シーザー暗号は安全か？

暗号文：ZHOFRPH WR XQLYHUVLWB RI BDPDQDVKL

- 上の例は**左に 3 文字**をずらすと解読される

平文：WELCOME TO UNIVERSITY OF YAMANASHI

- シーザー暗号であると分かれば、多くても **25 回の試行**で解読できる

暗号の基本用語

- 平文 : 伝えようとするメッセージ (第三者に知られたくない情報)
- 暗号文 : 第三者が分からないように平文を変換したもの
- 暗号化 (encryption) : 平文 x から暗号文 y を作ること

$$y = E(x)$$

- 復号 (decryption) : 暗号文 y から平文 x を復元すること

$$x = D(y)$$

- 任意の平文 x に対して, $D(E(x)) = x$ が成り立つ

例 : シーザー暗号

アルファベット A,B,...,Z を整数 0,1,...,25 に対応させると,

- $y = E(x) = x + 3 \pmod{26}$ (例: mod 26 で Y + 3 = B)
- $x = D(y) = y - 3 \pmod{26}$ (例: mod 26 で B - 3 = Y)
- 全ての x に対して $D(E(x)) = x$ が成り立つ

古典暗号から現代暗号へ

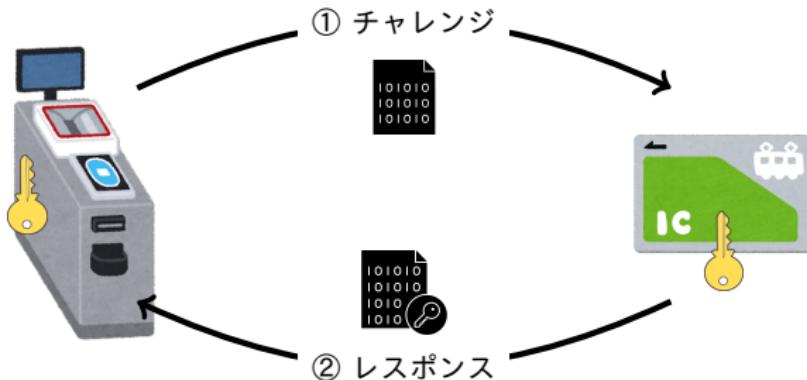
- 暗号化 (復号) アルゴリズム : 暗号化 (復号) するための操作手順
- 鍵 : 暗号化・復号のために必要な情報
- 共通鍵暗号方式 : 暗号化も復号も同じ鍵を使う暗号方式

	暗号化アルゴリズム	鍵
古典暗号 例：シーザー暗号	秘密 「右に k 文字ずらす」	秘密 「 $k = 3$ 」
現代暗号	公開	秘密

- 1970 年代以降、コンピュータ・インターネットの普及に伴い、アルゴリズムが公開される「標準暗号」が必要となった
- 1977 年にアメリカ連邦政府の暗号規格として DES (Data Encryption Standard) が採用された (現在では非推奨)
- 2001 年に DES に代わる新しい標準暗号として AES (Advanced Encryption Standard) が採用された

共通鍵暗号を利用した認証システムの例

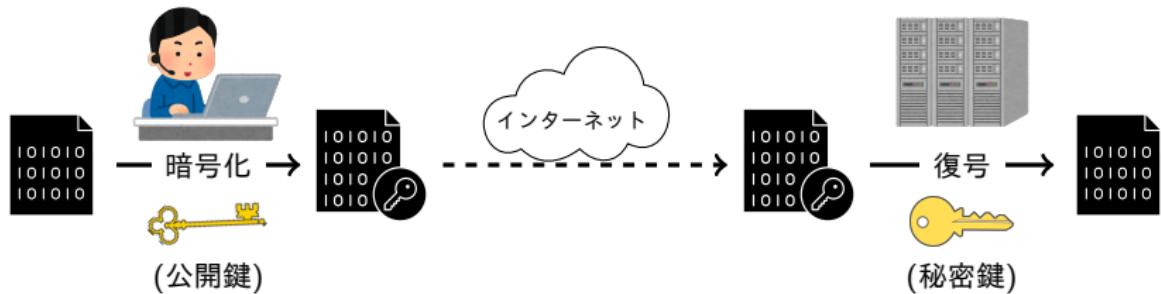
- ① 改札機（またはバス料金収納機）からランダムにメッセージ（平文）を発生させ、電波で IC カードに送信する
- ② IC カードの秘密鍵を使って受け取った平文を暗号化し、改札機に送信する
- ③ 改札機の秘密鍵を使って同じ平文を暗号化し、IC カードから受け取った暗号文と一致するなら、秘密鍵が一緒であることがわかる



共通鍵暗号 vs 公開鍵・秘密鍵暗号



共通(秘密)鍵暗号方式

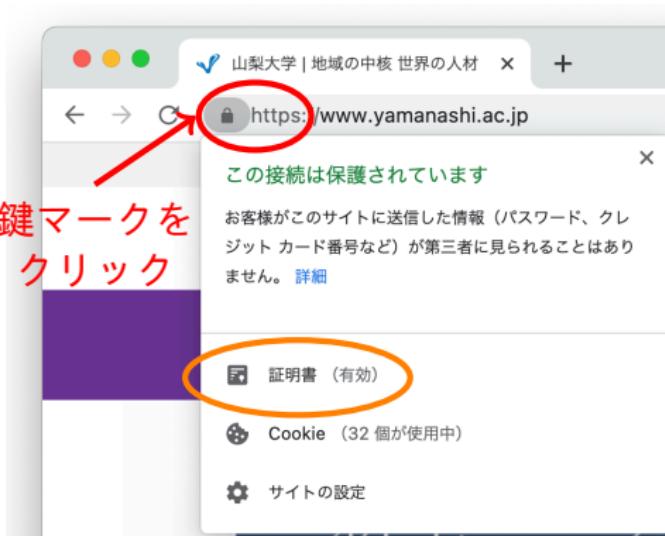


公開鍵・秘密鍵暗号方式(公開鍵暗号方式)

- 共通鍵を共有するために公開鍵暗号を利用することがある

インターネットにおける暗号の応用例：SSL/TLS

- **SSL/TLS¹**：インターネット上でデータを暗号化してやりとりする仕組みの1つ
- **HTTPS (HTTP² Secure)**：ウェブ通信を SSL/TLS を利用して暗号化してやりとりする仕組み



¹SSL: Secure Socket Layer; TLS: Transport Layer Security

²HTTP: Hyper Text Transfer Protocol

公開鍵証明書 (公開鍵暗号を広い範囲で使用する場合)

- 公開鍵とその正当な所持者の関係を証明するため、信頼できる第三者機関 (Trusted Third Party) に発行してもらう



公開鍵暗号の代表：RSA 暗号

ロナルド・リベスト アディ・シャミア レオナルド・エーデルマン

- 1977 年に Ronald Rivest, Adi Shamir, Leonard Adleman により提案
- RSA 暗号の貢献に対して、2002 年に計算機科学分野における最高の栄誉とされる「チューリング賞」受賞



左から Rivest, Shamir, Adleman (2003)

写真出典: <https://molecularscience.usc.edu/gallery-2/>

演習2：RSA暗号方式を体験しよう！

以下のウェブページにアクセスしてください

<http://www.kki.yamanashi.ac.jp/~xnlu/oc2022/>

- ①②③の順に RSA 暗号方式における「鍵の作成」「暗号化」「復号」を行ってください
- 秘密指数 d の値を変更して、もう一回「復号」してみてください
 - ①-3 の $d = \boxed{\quad}$ の中に他の数値を入力する
 - ③-6 の **秘密鍵 (N, d) を用いて復号する** を押す
 - ③ 復号したメッセージ³ を考察する

… 成功しない暗号解読

³各文字を Unicode (65535 以下の整数) に変換して演算したため、「文字化け」や☒(表示できない「文字」)になってしまうことがある

RSA 暗号方式の仕組み

① 公開鍵 (N, e) と秘密鍵 (N, d) を作成して公開鍵を公開する

- ▶ p, q : 異なる(大きな)素数 ; $N = pq$
- ▶ e (公開指数) : $r = (p - 1)(q - 1)$ と互いに素な整数
- ▶ d (秘密指数) : $de = mr + 1$ となる整数 (m : 整数)

② 平文 x ($0 \leq x \leq N - 1$) を暗号化する

$$E(x) = x^e \mod N$$

③ 暗号文 y ($0 \leq y \leq N - 1$) を復号する

$$D(y) = y^d \mod N$$

フェルマーの小定理により, $D(E(x)) = x$

$$D(E(x)) \equiv D(x^e) \equiv (x^e)^d = x^{de} = x^{mr+1} = (x^r)^m \cdot x \equiv 1^m \cdot x \pmod{N}$$

RSA 暗号の安全性

前提：非常に大きな N (実用上は 2048 ビット, 十進数では 617 衝) を利用

- 攻撃者 (悪意のある第三者) が秘密指数 d の取り得る値を 1 つずつ試すには、最悪の場合に 約 N 回試行 が必要
 - ▶ 128 ビット の N に対して、CPU のクロック周波数が 3GHz の PC を 80 億台使う場合に (1 クロックで 1 回の試行) 約 4496 億年⁴ が必要
- 公開の N と e を用いて d を推測できるか？
 $(de = m(p - 1)(q - 1) + 1)$
 - ▶ p と q が分かれれば d が効率良く求められる
- N を 素因数分解 さえすれば良いでしょう？
 - ▶ (現在のコンピュータで) 非常に巨大な整数に対して 効率の良い素因数分解アルゴリズムは知られていない

RSA 暗号は「計算量的安全」

(秘密鍵 d が漏洩しない限り) RSA 暗号解読に 膨大な計算量 が必要

⁴1 秒 3×10^9 回試行で $2^{128} / (3 \times 10^9 \times 60 \times 60 \times 24 \times 365 \times 8 \times 10^9) \approx 4496 \times 10^8$

秘密情報を守る秘密分散法

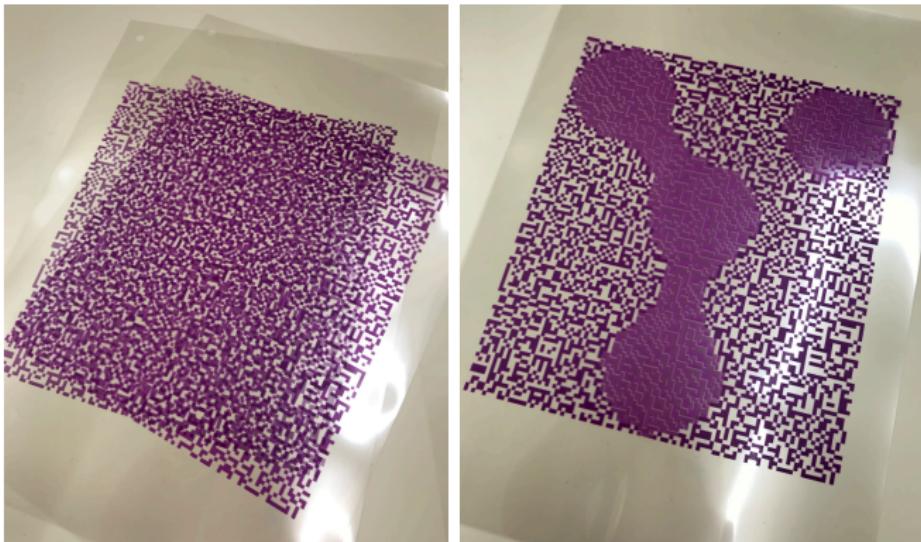
秘密情報（例えば秘密鍵）を守るためにどうすればいい？

- **秘密分散法**: 秘密情報を複数の**分散情報（シェア**という）に分けて管理し、必要なシェアを集めないと秘密情報を復元できない
- **秘密分散法**の実現には線形代数学、離散数学、情報理論、アルゴリズム論の知識が必要



視覚秘密分散法 (例 1)

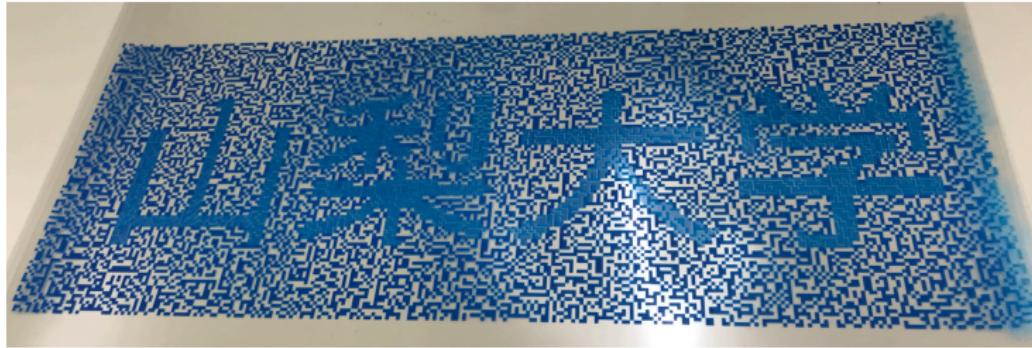
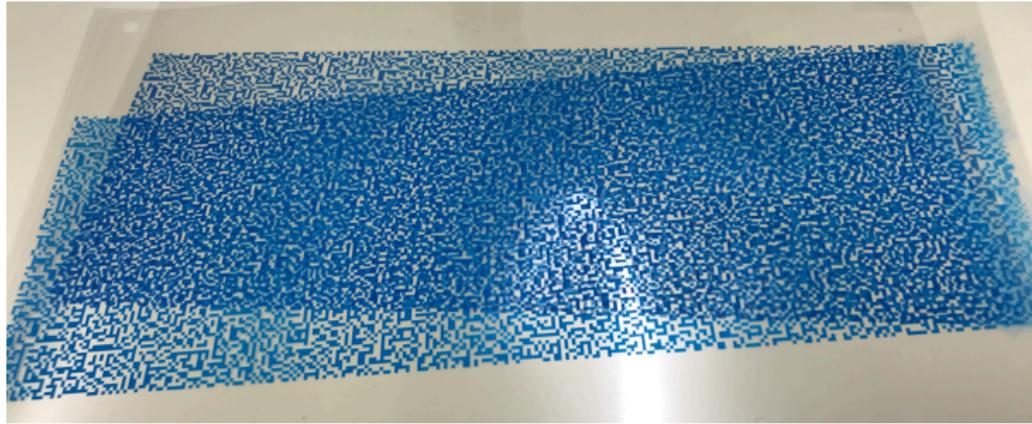
- 2枚のシェアを重ね合わせると次のように絵が現れる



視覚秘密分散法は「情報理論的安全」

1枚のシェアだけで無限のコンピュータリソース (計算能力) があったとしても秘密情報が復元できない

視覚秘密分散法(例2)



演習3：視覚秘密分散法を体験しよう！

以下のウェブページにアクセスしてください

<http://www.kki.yamanashi.ac.jp/~xnlu/oc2022/>

- 秘密の**文字列**（日本語も可）を入力して、2枚のシェアを生成し、そして**シェアを重ね合わせた結果**を確認してください
- 文字列の代わりに画像も適用できる。**山梨大学学章を生成する**や**山梨大学ブランドマークを生成する**を試してみてください
- **シェアを重ね合わせた結果**にマウスで指すと右の**拡大表示**に画面の拡大版が表示される
- シェアの色はいくつかの選択肢が用意されている。色が異なる2枚の**シェアを重ね合わせた結果**を**拡大表示**して考察してください

最新の暗号技術と将来の挑戦：耐量子計算機暗号

ショア

- 1994年に素因数分解問題を量子コンピュータで高速に解けるShorのアルゴリズムが提案された
- 量子コンピュータの性能が一定のレベルに到達するなら、RSA暗号等現在広く利用されている暗号技術は破られてしまう



- **耐量子計算機暗号** (量子コンピュータによる解読も耐えられる新たな公開鍵暗号) の理論研究・実用化が進められている
- 2016年より耐量子計算機暗号の標準化が始まり、2022年7月に暗号化方式1つ、デジタル署名方式3つが標準化された

写真出典: <https://www.ibm.com/jp-ja/quantum-computing> (日本初のゲート型商用量子コンピュータ「IBM Quantum System One」が2021年7月27日に始動)

冒頭の問題に戻ろう

- 以下の中に「暗号」(およびその応用)に当てはまるものは?



	(a) 合言葉	(b) 暗証番号	(c) マルウェア	(d) IC カード
守秘/認証	Yes?	Yes	No	Yes
暗号化	無	有	有?	有
復号/照合	無	有	無	有
安全性	-	弱	-	強
暗号?	✗	△	✗	○
セキュリティ?	△	○	○	○

ランサムウェア：マルウェアの一種であり、感染したコンピュータにシステムへのアクセスを制限したり、(使用できないようにするため)ファイルを暗号化したりする。制限を解除するため、被害者に身代金(ランサム)を支払わせようとする

まとめ

- ① (古典暗号) シーザー暗号の解読 … 安全性が弱い
- ② (現代暗号) 公開鍵暗号の RSA 暗号の体験 … 計算量的安全性
- ③ 視覚秘密分散法の体験 … 情報理論的安全性
- ④ 最新の暗号技術や将来の挑戦 … 量子コンピュータ時代の安全性

暗号技術・情報セキュリティの必要知識：

- 数学 (整数論, 代数学, 離散数学, 確率統計)
- アルゴリズム論, 計算量理論, 情報理論
- プログラミング, 計算機アーキテクチャ, ネットワーク, 情報倫理, 機械学習, IoT, ...

コンピュータ理工学科の教育・研究等については学科 HP へ

<http://www.cse.yamanashi.ac.jp/>