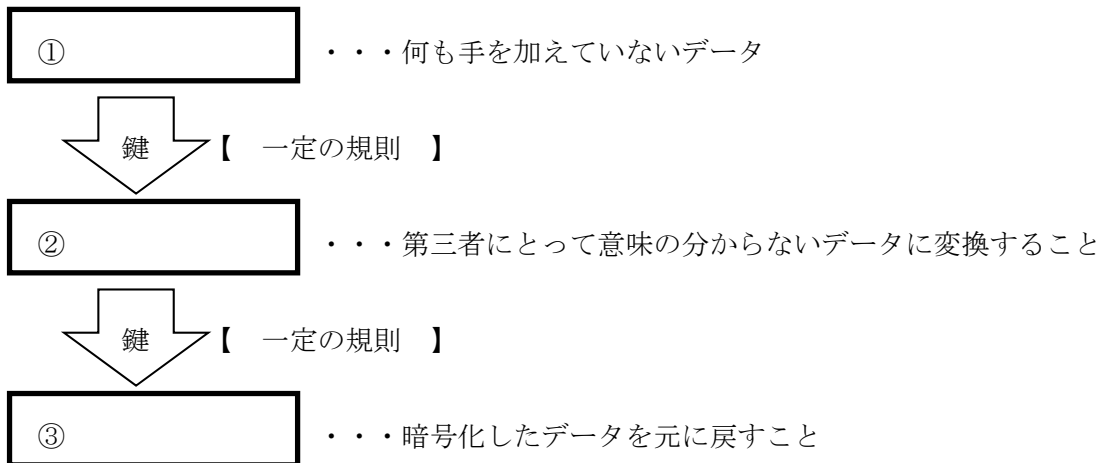


教科書 P. 128～ 情報の暗号化

1. 暗号化とは

機密性の高いデータは、第三者に悪用されないようにする必要がある



2. 暗号化の方法

④ ……暗号化と復号に同じ鍵の ⑤ を使用する方法

【実践1】シーザー・ローテーション

以下の暗号化された文字を別紙「資料1」を元に解読してみよう

いぼおふば ⇒

鍵【 】

※ 暗号化の鍵（ルール）を自分でも考えて、暗号文をつくろう

⇒

【メリット】

自分の考察
解答

【デメリット】

自分の考察
解答

⑥

・・・誰にでも教えてよい ⑦ で暗号化し、
自分だけが持つ ⑧ で復号する方法

【実践2】RSA暗号

[1. 平文] 数値の0～14（15種類）から好きなものを選択する

[2. 暗号化] (1) 自分の選択した数値を3乗する

今回の公開鍵のルール

(2) 上記(1)の答えを15で割り、余りをもとめる

(ア) 上記(1)の答えを15で除算した答えの
小数点以下を切り捨てた数値

(イ) 上記(ア)の答えを15で乗算し、(1)の
答えを減算した数値（マイナスはとる）

平文と違う数値になりましたか？

※ 以上の計算は「表計算ソフトウェア」を使用すると簡単に答えがもとめられる

[3. 復号] 先生がみんなの暗号化した数値を平文に復号します！

どうやったか【秘密鍵】

実は、暗号化された数値を

⑨

と平文に戻る

【メリット】

自分の考察

解答

【デメリット】

自分の考察

解答

3. ウェブページで用いられる暗号化

URLで「https://」で始まるページは、共通鍵暗号方式と公開鍵暗号方式、それぞれのメリットを活用した
組み合わせの ⑩ という方法で暗号化が行われている

どんな組み合わせ方？

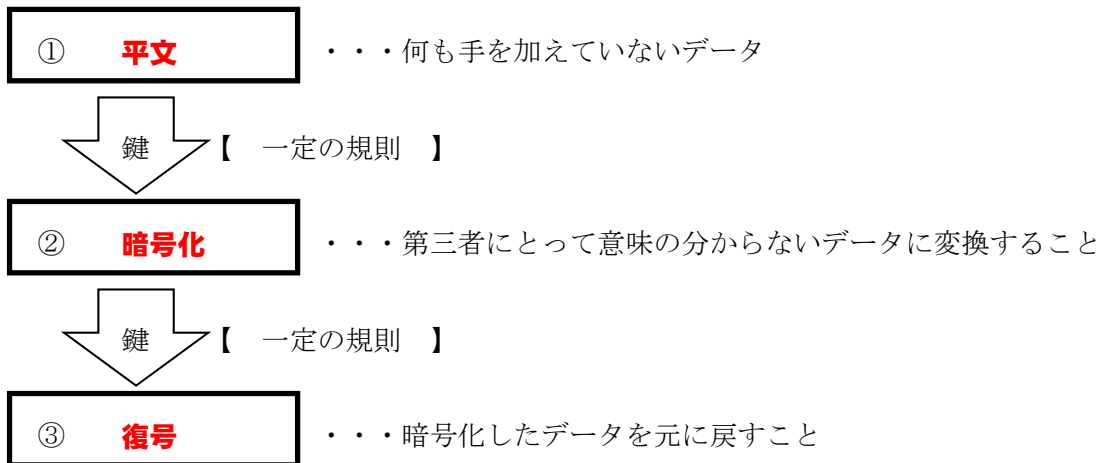
自分の考察

解答

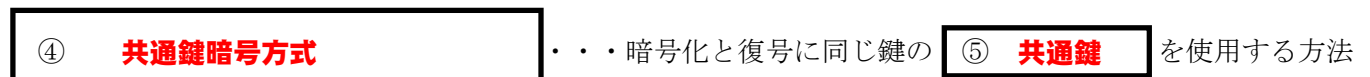
教科書 P. 128～ 情報の暗号化

1. 暗号化とは

機密性の高いデータは、第三者に悪用されないようにする必要がある



2. 暗号化の方法



【実践1】シーザー・ローテーション

以下の暗号化された文字を別紙「資料1」を元に解読してみよう

いぼおふば ⇒ 答え **せいしよう**

鍵【 **暗号化のときに、資料1の表で右斜め上に2マスずつ移動させている** 】

※ 暗号化の鍵（ルール）を自分でも考えて、暗号文をつくろう

暗号文 ⇒ 復号

【メリット】

自分の考察

解答

簡単に暗号化、復号ができる ⇒ 処理時間が短い

【デメリット】

自分の考察

解答

鍵（ルール）を相手に伝えるときに、第三者に知られる可能性がある

⑥ **公開鍵暗号方式**

・・・誰にでも教えてよい **⑦ 公開鍵** で暗号化し、
自分だけが持つ **⑧ 秘密鍵** で復号する方法

【実践2】RSA暗号

[1. 平文] 数値の0～14（15種類）から好きなものを選択する

[2. 暗号化] (1) 自分の選択した数値を3乗する

今回の公開鍵のルール

(2) 上記(1)の答えを15で割り、余りをもとめる

(ア) 上記(1)の答えを15で除算した答えの
小数点以下を切り捨てた数値

(イ) 上記(ア)の答えを15で乗算し、(1)の
答えを減算した数値（マイナスはとる）

平文と違う数値になりましたか？

※ 以上の計算は「表計算ソフトウェア」を使用すると簡単に答えがもとめられる

[3. 復号] 先生がみんなの暗号化した数値を平文に復号します！

どうやったか【秘密鍵】

実は、暗号化された数値を

⑨ 7乗して、15で除算して余りをもとめる

と平文に戻る

【メリット】

自分の考察

解答

復号する鍵（ルール）を誰にも伝えないので、平文を第三者に知られることがほぼない

【デメリット】

自分の考察

解答

暗号化・復号の計算が大変 ⇒ 処理時間が長い

3. ウェブページで用いられる暗号化

URLで「https://」で始まるページは、共通鍵暗号方式と公開鍵暗号方式、それぞれのメリットを活用した組み合わせの **⑩ SSL** という方法で暗号化が行われている

どんな組み合わせ方？

自分の考察

解答

共通鍵を公開鍵暗号方式で相手に伝え、その後、共通鍵暗号方式でデータのやりとりをする