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

①　　・・・何も手を加えていないデータ

鍵【　一定の規則　】

②　　・・・第三者にとって意味の分からないデータに変換すること

鍵【　一定の規則　】

③　　・・・暗号化したデータを元に戻すこと

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　　⇒　答え

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

暗号文　　⇒　復号

【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］
今回の公開鍵のルール
（１）　自分の選択した数値を３乗する
（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

① **平文** ・・・何も手を加えていないデータ

鍵【　一定の規則　】

② **暗号化** ・・・第三者にとって意味の分からないデータに変換すること

鍵【　一定の規則　】

③ **復号** ・・・暗号化したデータを元に戻すこと

２．暗号化の方法

④ **共通鍵暗号方式** ・・・暗号化と復号に同じ鍵の ⑤ **共通鍵** 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　⇒　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］

今回の公開鍵のルール

（１）　自分の選択した数値を３乗する

（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**