(Updated 2020/07/30)(更新 7/25)(作成 2020/04/25)
「説明資料 PDF(rsasetsumeippt2020.pdf(ppt))の解説資料」scriptsetsumei2020.pdf(docx)

p.1
本実験項目は、「情報通信（情報セキュリティ)」というタイトルです。
内容は、「暗号の理解とプログラミング」で、具体的な暗号として RSA 暗号を扱います。

p.2
本課題の資料は、本課題の web 上においてあります。
１．これから説明に使う資料は、この説明資料（rsasetsumeippt2020.pdf）です。
２．この説明資料の元となる課題テキストは、rsatext.pdf になります。
３．そして、これらを含む他の資料は本課題の web ページである、この URL（http://www.code.cei.uec.ac.jp/Class/jikken-cei/index.html）にあります。

p.3
ここに示す図は、「デジタル通信システム」における主な「符号化」です。
まず、「送信側」と「受信側」の 2 者が、「通信路」でつながっています。
「通信路」とは、無線、光ケーブル、LAN ケーブルなどです。
大きな枠組みでは、インターネット、電話、衛星通信、衛星放送などの通信のことです。
「情報源」から出るデータは、まず、「効率性」を目的として、「データ圧縮」が行われます。
これを「情報源符号化」といいます。
次に、「安全性」を目的として、「暗号化」が行われます。
そして、最後に、通信路での雑音に耐えるために、「信頼性」を目的として、「誤り訂正符号」による「通信路符号化」が行われる。
ここまでがデジタル処理です。
ちょうど、青枠で囲まれているのが、3 種類の符号化になります。

実際の通信路は、物理的なアナログ通信路ですので、「符号化変調」というもので、デジタルデータをアナログデータに変換します。
そして、そのアナログデータを通信路に送信します。
「受信側」では、受信したアナログデータを「符号化復調」でデジタルデータに変換します。
そして、送信側が行った「符号化」の手続きに対応する「復号化」の手続きを実行します。
この手続きにより、受信側は、元のデータを復元することができる、という仕組みです。

以上が、デジタル通信システムのおける主な符号化です。

p.4
本課題のテキストの構成内容です。
1 節は、本実験の目的である以下の 2 点が書かれています。
　１．RSA 暗号の暗号化と復号化の方法について理解する。
　２．RSA 暗号の暗号化と復号化のプログラムを作成する、です。
2 節は、提出していただくレポートの内容です。
必ず、テキストの 2 節の内容を確認して下さい。
3 節は、はじめにとして、本テキストの趣旨と RSA 暗号の出典について書かれています。
そして、4 節では、暗号化として、次の 3 点を説明しています。
　4.1 節は、導入として、具体的な暗号としてシフト暗号について説明します。
　4.2 節は、暗号化システムを特徴付けるための形式的記述というものが説明してあります。
　4.3 節は、主な二つの暗号システムとして、公開鍵暗号と秘密鍵暗号（共通鍵暗号）を説明します。
５節は、RSA 暗号で使う整数に関する諸性質が書かれていますが、高校や大学 2 年生までにすでに学習した事柄です。
したがって、最初から読む必要はなく、必要なときに確認として読めばよい内容として記載してあります。
そして、6 節に、公開鍵暗号の一種となる RSA 暗号について、鍵の生成、暗号化、復号化について説明します。
７節は、本課題で要求される課題プログラムについて書いてあります。
必ず、中身を確認し、何を要求されているのかを理解した上で、プログラミングの作業を始めて下さい。
最後の８節では、課題のプログラムを作成するに当たり、参考となるプログラミングについて書いてあります。
以上が、テキストの主な内容です。
この説明資料でも上記の順に、必要な項目だけについて説明をします。

p.5
本課題で要求する提出レポートの内容です。
成績評価は、主に提出レポートで評価しますので、必ず、テキストの 2 節の内容を確認して下さい。

ｐ.6
はじめに。
ここに書いてある通りです。

読んでください。

p.7

暗号化。

ここでは、皆さんが、一般的に想像する暗号の仕組みについて説明します。

まず、図では、A さん、B さん、C さんの三者がいます。

A さんは B さんに、メッセージを伝えたい。

ただし、第三者の C さんには、その内容を知られたくない、とします。

そのために、図に示すように、暗号化の鍵を用いて、メッセージから暗号文を生成します。

そして、通信路を介して、暗号文を B さんに伝えます。

B さんは、復号化の鍵を用いて、元のメッセージを復元します。

一方、C さんは、通信路を盗聴し、暗号文を入手できますが、復号化の鍵がないので、暗号文を復元できない、というのがこの図です。

このためには、鍵の情報を、A さんと B さんが、C さんには知られないように共有する必要がある、ということが重要になります。

メッセージを送る前に、鍵を共有する必要がある、ということです。

p.8

それでは、前頁の図に対応するような具体的な暗号として、シフト暗号を説明します。

１．まず、扱うデータとして、「メッセージ集合と暗号文集合」というものを考えます。

いずれも、26 文字の大文字の英字で構成されるとします。

２．「暗号化と復号化の方法」は、循環シフトです。

ここでは、鍵となる情報を整数 k とします。

すると、暗号化は、辞書順にしたがって、右に k だけ循環シフトさせる変換です。

復号化は、逆に、左に循環シフトさせます。

３．鍵 k=5 として、循環シフトの具体例を以下に示します。

メッセージ「H」を伝えたい場合は、暗号文「M」を送ります。

また、「W」を伝えたい場合は、「B」を送ります。

「Z」の次が「A」であるところが「循環」という意味です。

復号はこの逆になります。

p.9

この頁(ページ)の図は、鍵 k=5 として、
メッセージ「WEWILLMEETATCHOFUSTATION」
を伝えたい場合は、各文字を右に k=5 の循環シフト変換させた
暗号文「BJBNQQRJJYFYHMTKZXYFYNTS」
を送信するというものです。

p.10
「算術演算を利用しよう」
ここでは、「シフト」という操作を「算術演算」に置き換えることを考えます。
これは、扱うデータを「文字」から「整数」にするということになります。
なぜ、そのように考えるのかというと、コンピュータでのデータ処理を考えると、シフトという操作よりも、算術計算の方が高速に処理できるからです。

そこで、ASCII（文字コード）を利用します。
例えば、ASCII の表から、大文字の「A」は図のように表されています。
その結果、「A」を 10 進数で表すと「65」になります。

p.11
「文字」から「整数」への対応を考えると、次の表のようになり、「文字の集合」は「整数の集合」に対応させて考えることができます。
さらに、合同関係を考えると、「整数の集合」の要素を 26 で割った「余りの集合」も同様に対応させて考えることができます。
「文字」「整数」「余り」の対応は表のとおりです。

「シフト処理」から「算術演算処理」への例は、次のとおりです。
「 H を右に 5、循環シフトし、M に変換」というシフト処理は、「 72 に 5 を足した 72+5=77 」という算術演算処理になります。
次の循環シフトの例の場合も同様です。
「 87+5=92 」ですが(mod 26)では、「 92=66 (mod 26)」となりますので、問題なく暗号文を作れることを確認できます。

p.12
算術演算処理によるシフト暗号の例は以下のようになります。
メッセージ「WEWILLMEETATCHOFUSTATION」
は整数の

　メッセージ「87 69 87 73 76 76 77 69 69 84 65 84 67 72 79 70 85 83 84 65 84 73 79 78」
になります。そして、暗号化すると
　暗号文「66 74 66 78 81 81 82 74 74 89 70 89 72 77 84 75 90 88 89 70 89 78 84 83」
になります。

図で注意する箇所は、暗号化と復号化の手続きを「算術演算」として表現できているところです。

別の注意として、空白(スペース)は暗号文集合にはありませんので、本来の暗号文は「667466788181827474897089727784759088897089788483」となります。
区切り記号がないと、復号するとき、どの数字を取り出せばよいか分からなくなります。
しかし、この場合は、すべてのデータが 2 桁であるため、2 桁ずつ取り出すという規則で対応できます。
つまり、区切り記号がなくても、データを固定長で扱えばよいことが分かります。

以上までが、暗号についての導入部分となる、具体例のシフト暗号の説明になります。
次は、二つの暗号化システムについて説明します。

p.13
暗号化のシステムを大きく二種類に分類すると
　「秘密鍵暗号システム（共通鍵暗号システム)」
と
　「公開鍵暗号システム」
になります。

先ほど、説明したシフト暗号は、前者の秘密鍵暗号システムになります。
一方、本課題で扱う RSA 暗号は、後者の公開鍵暗号システムになります。

p.14
この頁では、「秘密鍵暗号システム（共通鍵暗号システム)」について説明します。
１．暗号化鍵 K を第三者に秘密にするためには、図に示すような「安全な通信路」を利用する必要があります。
もし、そのような安全な通信路というものがあれば、その安全な通信路を利用してメッセージを送ればよいことになります。
しかし、一般には、そのような安全な通信路を確保して、利用することは難しいと考えられます。

利用することが難しい、という表現に関連し、効率が良くない、ということことも考えられます。
２．鍵については、A さん、または、B さんのどちらでも生成することが可能です。
それは、生成した方が、相手に安全な通信路を利用して送ればよいからです。

最後に、秘密鍵暗号システムでの問題点は、鍵を共有しなければいけないということになります。

p.15
この頁では、「公開鍵暗号システム」について説明します。
１．図に示すように、暗号化用の鍵は、「公開鍵」と呼ばれ、一般に、公開することができます。
つまり、第三者の C さんを含め、誰でも、暗号化鍵を入手できるということです。
２．そのため、鍵の受け渡しが必要なくなり、安全な通信路を利用する必要がありません。
３．ただし、図に示すように、暗号化する鍵と復号化する鍵は、異なる必要があります。
さらに、暗号化鍵から、復号化鍵（秘密鍵という）を容易には推測できないようになっている必要があります。
これが、安全性に関わる必要な条件の一つになります。
４．図のシステムでは、暗号文を受信する側の B さんが暗号化鍵と秘密鍵をペアで生成します。
そして、暗号化鍵だけを公開します。
５．最後に、RSA 暗号は、図に示すシステムを実現する公開鍵暗号システムになります。

繰り返しになりますが、公開鍵暗号の特徴は、「暗号化と復号化の鍵が異なる」ということと、「その鍵のペアは、受信側が作成する」ということになります。

p.16
先に述べた二種類の暗号システムの違いについて、まとめます。
1 点目は暗号化鍵と復号化鍵が、同じものか、異なるのかということです。
2 点目は鍵を誰が作成するのかということです。

p.17
「RSA 暗号」
先ほどまでに説明したように、RSA 暗号は公開鍵暗号の一種です。
１．そこで、まず、はじめに、鍵の作成方法について説明します。
　そのためにいくつかの整数を選択し、計算します。

１．互いに異なる素数 p と q を選びます。
２．そして、それらの積を n=pq とします。
３．次に、(p-1)と(q-1)の最小公倍数を L=lcm((p-1),(q-1))とします。
４．そして、そのＬと互いに素で、1< e <L　を満たす整数 e を選びます。
　一般に、このような e の候補は複数ありますので、その中から選ぶことになります。
５．最後に、上記までに述べた e とＬに対し、e*d=1(mod L)を満たす整数 d を求めます。
　この d は、(mod L) で考える上では、一意に定まります。
　つまり、1個しか存在しないということです。

２．上記の手続きで生成した整数を情報として、公開鍵と暗号化鍵は次のようになります。
１．公開鍵(e,n)
２．秘密鍵(d,n)
３．そして、鍵を生成した者が秘密にしておくべき情報は(p,q,L,d)となります。
　　これらの情報のどれかが洩(も)れると、公開鍵の情報から秘密鍵を推測しやすく、または、推測されてしまうからです。

p.18
１．この頁では、(p,q)=(5,11)を選んだ場合の鍵作成の例を示します。
作る手順は示した通りです。
項目４で e=7 を選ぶ。
項目５で、d=3 を求めています。
このとき、表で示すように、(mod L=20)で考えるので、d の取る整数の範囲は 1 から 20 まででよいことを理解して下さい。
そして、その中で一意に d=3 と決まることを確認して下さい。

２．このとき、公開鍵や復号化鍵は以下のようになります。
１．公開鍵(e,n)=(7,55)
２．秘密鍵(d,n)=(3,55)
３．そして、鍵を生成した者が秘密にしておくべき情報は(p,q,L,d)=(5,11,20,3)となります。

p.19
後の説明用に、(p,q)=(17,19)の場合の鍵生成の例をこの頁に示しておきます。

p.20

鍵（公開鍵と復号化）の作成については、前頁までに終えました。

この頁では、その鍵を用いて、どのように暗号化と復号化を行うのかを説明します。

１．公開鍵(e,n)用いて、メッセージ(整数) M を暗号化し、暗号文 C を生成するには、このように、(mod n)におけるべき乗の計算をします。

２．復号化は、復号化鍵(d,n)を用いて、暗号文 C をメッセージ M に復元するには、符号化と同様に、このように、(mod n)におけるべき乗の計算をします。

３．最後に、元のメッセージと、復元したメッセージが等しい理由は、この式が成り立つことによります。

この式の証明は、この課題で説明する範疇外になりますので、興味のある学生は各自で調べるとよいと思います。

p.21

「RSA 暗号を用いた公開鍵暗号システム」

この頁は、RSA 暗号の場合のシステムの図を示したものです。

注意するところは、「暗号化と復号化の演算処理が RSA 暗号のべき乗の計算」になっているところと、「暗号化鍵と復号化鍵が異なる」ところです。

具体的な暗号化と復号化の例では、以下のようになります。

１．大文字の「C」を暗号化することを考えます。

「C」は 10 進数で「67」ですので、公開鍵(5,323)でのメッセージ「M=67」の暗号文は「C=67^5=288 (mod 323)」となります。

メッセージの「C」と暗号文を表す「C」が同じでまぎらわしいですが、資料では少しフォントの違いがありますので、区別して下さい。

どうしても、公開鍵(5,323)に対し、メッセージの「C」がちょうどよい例になるためにこの例を使っています。

２．復号化鍵(29,323)で暗号文「C=288」を復元すると「M=(288)^(29)=67 (mod 323)」となり、元のメッセージを得ることができる。

ここで、注意としては、整数のべき乗の計算はとても大きな値になります。

実社会で利用されている RSA 暗号で扱う整数と比較すれば、本実験で扱う整数は小さい値であるが、C 言語のべき乗計算の関数 pow では正しく計算できない可能性がある。

したがって、べき乗の計算についてプログラムを書く場合には、注意が必要である。

テキストの「例 6.2」や「8 節 プログラミング」の説明を読んで下さい。

p.22
この頁では、暗号化鍵(e,n)=(5,323)を用いて
　メッセージ「WEWILLMEETATCHOFUSTATION」
を暗号化する例を示してあります。

表示してある
　暗号文:「83 103 99 247 247 229 103 103 50 12 50 288 21 129 185 187 87 50 12 50 99 129 108」
は、メッセージの各文字毎に対応できるように空白で区切られている。
しかし、この区切りがないと
　「8310399247247229103103501250288211291851878750125099129108」
となる。
これでは、どの数字を復号すれば分からなくなる。
したがって、プログラムを作成するときには、空白での区切りと同じような役目を得るために固定長でデータを扱う、保存するということを考える必要がある。
「8 節 プログラミング」に説明がありますので読んで下さい。

p.23
「7 節 課題」
課題として、7 個の課題があります。
詳細については、必ず、テキストの 7 節を読んで、要求されていることを理解した上でプログラムを作成して下さい。

課題１は、次に示すような要件を満たす RSA 暗号の暗号化、復号化のプログラムを作成せよ、という内容です。
暗号化のプログラムは、「暗号化鍵とメッセージファイル」を入力すると、「(メッセージが) 暗号化されたファイル」を出力するというプログラムということです。
復号化のプログラムも同様の仕様です。

課題２は、例 6.3 に示した 2 進展開法というべき乗の高速計算アルゴリズムを採用した RSA 暗号のプログラムを作成せよ、という内容です。
この課題は、課題１で作成した RSA 暗号プログラムのべき乗計算に関わる部分を修正すれば、作成できるはずです。

課題３は、課題１と２で作成した処理速度の異なるプログラムを実行して、実際の計算時間がどのようになるのかを計測し、そのデータを表とグラフに表しなさい、というものです。
また、その計測データが、理論的な時間計算量と比較して、妥当な結果になっているかも確認して下さい。

課題４から７は、暗号化と復号化の処理とは別で、暗号化と復号化の鍵のペアを作成する場合に利用できるプログラムを作成せよ、というものです。

繰り返しになりますが、テキストの 7 節の各課題をしっかり読んで下さい。

p.24
最後に頁になります。
テキストの 8 節のプログラミングです。
　8.1 節は、プログラムを作成する上での準備のようなことが書かれています。
　8.2 節は、RSA 暗号の動作の例として、参考プログラムの入出力を示してあります。

その他の参考プログラムとして、本課題の web 上に以下のものがあります。
１.「「参考資料」→「参考プログラムの説明」」には、参考プログラム(ソースファイルや実行ファイル)とその使い方や入出力結果を示してあります。
２.「「参考資料」→「課題１ のプログラムを作成するためのヒント(練習プログラム)」」には、課題１を作成するためのヒントが書かれています。
記載とおりに作業をすすめると、最後に、RSA 暗号の符号化、暗号化のプログラムを完成できるように指示してあります。
RSA 暗号を作成する上で、どのように作業を進めればよいか分からない場合は参考になると思います。

以上で、rsasetsumeippt2020.pdf の各頁の解説は終わりです。

(遠隔授業対応として軽量データサイズの資料作成 scriptrsasetsumei2020.docx)

電気通信大学 情報理工学域 II 類 情報通信工学プログラム/電子情報学プログラム
2020 年度後期
情報通信工学実験 B / 電子情報学実験 B
実験課題「情報通信（情報セキュリティ）」