暗号の数理要綱 #5

2 公開鍵暗号

2.1 暗号に関する用語

暗号 (*cryptography*) とは，普通の文章を第 3 者が理解できないような文字列に変換することである。

まず，用語の定義から。

定義 2.1 (1) **文** とは，文字の列のことである。

(2) **文字** とは，いくつかの記号の集まりのことであり，その集まりの中で，個々の記号もまた文字という。

(3) 文字には，英語のアルファベットや日本語の漢字，ひらがな，カタカナ以外にも，世界中に多くの文字があり，また，空白，ピリオドや改行コード，タブなどの制御コードなどが含まれることもある。

どのような場合にせよ，これらは有限個の記号の集まりであり，$0 \sim N-1$ という N 個の数字に置き換えることができる。以下では，**アルファベット** と言ったら，ある文字の集まりか，あるいは，$0 \sim N-1$ という N 個の数字の集まりを指す場合がある。

(4) 普通の文 (暗号化されていない文) を **平文 (ひらぶん)**(*plaintext*) という。

(5) 何らかの方法で変換された結果できた文を **暗号文，暗号化文** (*ciphertext*) という。

(6) 平文を暗号文に直す操作を **暗号化** (*encryption*) と言う。

(7) 暗号文を元の平文に直す操作を **復号化** (*decryption*) と言う。

(8) ある文字の平文を暗号化によって別の文字の暗号文に変換するということが考えられるが (例えば英語の文を漢字の列に直すなど)，最初からこれら 2 種類の文字の全体を一つの文字の集まりであるとしておけば良いので，暗号化に使用する文字は，1 種類であると仮定しても問題はない。

(9) $\Sigma = \{0, \cdots, N-1\}$ を文字とし，これを文字とする文全体の集合を $\mathcal{T}$ とする。 すなわち，$\mathcal{T}$ は Σ の元の有限列全体である。長さ M の文字列全体を $\mathcal{T}_M$ で表す。

(10) M を一つ決め，$\mathcal{T}_M$ を考える。$\mathcal{T}_M$ からそれ自身への写像 $f : \mathcal{T}_M \to \mathcal{T}_M$ で全単射であるものを**暗号化変換**と言い，その逆写像 $f^{-1} : \mathcal{T}_M \to \mathcal{T}_M$ を**復号化変換**という。

(11) ある文字列 K_E によって暗号化変換 f が定まる時，その文字列 K_E を，暗号化の**鍵** (*key*) という。同様に， ある文字列 K_D によって復号化変換 f^{-1} が定まる時，その文字列 K_D を，復号化の鍵という。

2.2 暗号化の方法

2.2.1 換字暗号 (substitution cipher)

最も簡単な暗号は，それぞれの文字を別の文字で置き換える，というものである。すなわち，アルファベット Σ の各元に別の元を対応させることにより暗号化される。

具体的には，$\alpha : \Sigma \to \Sigma$ を Σ からそれ自身への全単射とすると，文章 $t = t_1 \cdots t_n \in \mathcal{T}$ に対して，$\alpha(t_1) \cdots \alpha(t_n) \in \mathcal{T}$ を対応させることにより，暗号化される。ここで， t_i は Σ の元であり，文字を表す。

例 1．カエサル (シーザー) 暗号： Julius Caesar は，アルファベットの文字を 3 文字ずつずらすことにより，文章を暗号化したと伝えられている。すなわち，アルファベット $\{A, \cdots, Z\}$ を $\{0, \cdots, 25\}$ と同一視すると，暗号化変換 $f : \mathcal{T} \to \mathcal{T}$ は，各文字 t_i に対して $f(t_i) = t_i + 3 \mod 26$ を対応させる写像となる。

例えば，

“ pdb wkh irufh eh zlwk brx ”

という文は，ちょっと見ると全くわからないが， $\mod 26$ で -3 を加えることにより簡単に復号化される。

同様にして d 文字ずらす，ということで，25 通りの暗号化ができる (0 文字シフト，26 文字シフトは，何もずらしていないので，暗号にならない)。

このように，暗号というものを良く知らない相手に対しては，この程度の単純なものでも，結構役に立つのかもしれない。

シフトではすぐに破られてしまうので，もっと複雑な換字暗号も考えられる。一般に N 文字のアルファベット (例えば英語なら $N = 26$ またはピリオドなどの記号を入れて 27 またはそれ以上) に対し適当に別の文字を対応させることもできる。

例 2．強化された換字暗号： しかし，単なるアルファベットのシフトでは key が $N-1$ 通りしかないので，敵が暗号についての知識を少し持っているだけで簡単に破られてしまう。そこで，もう少し複雑なルールでアルファベットを別のアルファベットに対応させることを考える。

各アルファベットに適当に別のアルファベットを対応させることも考えられるが，これでは暗号を使用するとき，対応表を持っていなくてはならず，対応表が暗号解読者の手にはいる可能性もある。

そこで次のような key word による換字暗号が考案された。key word をたとえば「暗号の数理」と「X」だとして説明しよう。「暗号の数理」をローマ字で書き重複するアルファベットを消去する。

暗号の数理 $\longrightarrow$ angounosuuri $\longrightarrow$ angousri

１行目はこの「angousri」から始め i の次は前に出てきてないアルファベットを順に書いていく。この例で言うと，i の次は j, j の次は k と書いて行き，n が出てきたらそれは飛ばす。z まで行ったら a に戻る。それを 1 行目とし，2 行目は X から順に書いていく。この場合

a n g o u s r i j k l m p q t v w x y z b c d e f h
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

という対応表が作れる。これを見ながら暗号化し，暗号化終了後この対応表を燃やせばよい。

換字暗号の解読：

- key がある程度少ないと，全ての場合をチェックすることにより，解読されてしまうので，実際上は実用にならない。
- また，一つの key で多くの文を送ると，文字の **出現頻度解析** などにより破られてしまう可能性がある。
- Key の可能性が非常に多く，また文がそれほど長くないならば，統計的な効果が出ないので，破るのは非常に難しくなる。
- どちらにせよ，文字の間の **規則的な対応関係** がある場合には，その規則が暗号文に現れてしまい，解読されてしてしまう。
- **何の規則もない暗号** というのが，最も解読が難しい暗号である。(**One time pad**)

2.2.2 ブロック暗号

定義 2.2 (1) n 個の文字の列を，長さ n の **word** という。すなわち word とは， Σ^n の元とみなすことができる。

(2) 文は，文字の列を n 個ごとに区切ることにより，長さ n の word の列とみなすことができる。長さ n の word に対して，別の長さ n の word を対応させることにより，文を暗号化できる。これを **ブロック暗号** という。

(3) アルファベットの各文字を数字に対応させ，さらにその数字を 2 進数表示することにより，全ての word は $\{0,1\}$ の列と見なすことができる。すなわち，ブロック暗号に関しては，アルファベットとしては，$\{0,1\}$ だけを考えれば十分である。

(N-個の文字から成るアルファベットの換字暗号も，それぞれの文字が $\{0,1\}$ の列であると見なせば，$\{0,1\}$ という 2 つの文字からなる文のブロック暗号であると見なせる。)

例。アファイン線形ブロック暗号： $w \in \Sigma^n$ を長さ n の word とする。A を Σ の元を成分とする n-次正方行列とし，$b \in \Sigma^n$ とする。$f : \Sigma^n \to \Sigma^n$ を

$$f(w) = Aw + b$$

によって定義する。これにより，長さ n のブロックを暗号化できるが，このままでは復号化できるとは限らない。

$$f^{-1}(v) = A^{-1}v - A^{-1}b$$

でなければならないので，A に対して，その逆行列 A^{-1} が定義されなければならない。

一般に，正則行列 A に対して，その逆行列は，$adj\ A$ を A の余因子行列とした時，

$$A^{-1} = \frac{1}{\det A}\, adj\ A$$

となる。

アルファベット Σ の文字数が N の時，全ての演算は $\mod N$ で行われる。余因子行列 $adj\ A$ の成分は，単に A の成分の和と積のみで表されるので問題はない。$\det A$ が $\mod N$ で逆元を持つかどうか，ということが問題となる。これに関しては，$\det A$ を含む剰余類が

既約剰余類であれば逆元を持つので，$\det A$ が N と互いに素の場合に，A は逆行列を持つことになる。

以上から，暗号化写像 f を定義するための行列 A として $\det A$ が N と互いに素となるものをとれば，f は復号化写像 f^{-1} を持つことになる。

特に $N = 2$ の場合，$\Sigma = \{0, 1\}$ であり，$\det A = 1$ の場合に限り，A は逆行列を持つことになる。

アファイン線形ブロック暗号の key は，(A, b) であり，復号化鍵は $(A^{-1}, A^{-1}b)$ となる。

実際のブロック暗号は，文字列を変換する操作を複雑に組み合わせて構成され，解読が極めて困難であるようなものとなっている。しかしその操作は基本的に，word の入れ替え，置き換えや，行列による変換などであり，暗号化，復号化が高速にできるのが特徴である。

かつてのアメリカの標準的暗号システムである **ＤＥＳ** や，2000 年に認定された現在の標準的暗号システムである **ＡＥＳ** などもブロック暗号の一種である。

2.3 公開鍵暗号

上で述べたような暗号システム，すなわち 1970 年代まで使われていた全ての暗号システムにおいては，暗号化された文書を解読するための鍵を，受信者はあらかじめ知っていなければならない。

Abel が Briskorn に文書を暗号化して送る場合を考えてみる。(暗号理論の説明で最も標準的に使われている名前は Alice と Bob であるが数学者の名前に変えてみた。)

あらかじめ暗号化の方法については合意していたとしても，Briskorn は Abel がどのような key で暗号化したのかを知らないと解読はできない。そのため，Abel は Briskorn に対して，解読のための key を何らかの方法で送る必要がある。しかし，全ての通信が傍受されている可能性がある中で通信を行おうとする時，解読 key の交換は極めて危険である。

以前のように，暗号通信を必要とする者が，一部の政府機関や軍事組織などに限られていた時代であっても，key の配送というのは大きな問題であった。暗号通信は，遠く離れた者同士で行われるのが普通なので（近くの者同士は，直接会って話すのが最も安全である），遠くにいる相手まで，key を安全に届けなければならない。Key を通信で送ることはできないので，誰かが直接配送しなければならないのである。

第 2 次世界大戦の段階ですでに，暗号解読の成否が，戦況を大きく左右していた。解読を防ぐためには key を頻繁に変更する必要があったが，戦地に展開している全ての部隊に対して key を配送するのは，大変な労力を必要とし，また一歩間違えば，途中で敵に key が奪われるという，大きな危険も付きまとう。

このように,「鍵配送問題」というのが，暗号に付随する最も大きな問題であったが，軍隊や政府機関，大企業，銀行などは，たとえ経費がかかったとしても，それを行うだけの力を持っている。実際に銀行などでは，暗号通信を必要とする多くの取引先に対して，信頼された特別な配送人が実際に赴いて，直接鍵を手渡していたのである。

しかし，大量の情報がネットワークを通して流れる時代になると事態は変わってくる。経済活動や公式書類の電子化にに関連して，多くの者が秘密情報を暗号化して送る必要が生じてくる。そして通信を行う者同士は，それまで会ったこともなければ，key を交換するためにどこかで落ち合う

ような時間的余裕もない。また，ネットワーク通信というものは，多くのコンピューター，通信会社などを経由しており，そのあらゆる経由地点において，第 3 者による通信傍受の可能性が存在する。

このようなネットワーク社会における膨大な量の暗号化通信において，誰かに頼んで相手まで key を直接届けてもらうというような方法が，全く役に立たないことは言うまでもない。本質的に異なる新たな方法が必要であることは明らかだった。

1976 年，そのような鍵配送問題に取り組んでいたスタンフォード大学の Whitfield Diffie と Martin E. Hellman は，それまでのものとは全く異なる画期的な方法を思いついた。それが**公開鍵暗号**である。

(“New direction in cryptography” Trans. IEEE on Information Theory, IT-22, No.6, 644-654 (Nov. 1976))

この方法の本質は，暗号通信において，**公開鍵** (*public key*) と**秘密鍵** (*secret key*) という 2 つの key を設定した点にある。

- 文書を暗号化したい者は，自分自身の公開鍵と秘密鍵を作成する。
- 公開鍵は他の者が知ることができる形で公開する。秘密鍵は，他の者が知ることができないような形で保管する。
- 平文は，公開鍵で暗号化することもできるし，秘密鍵で暗号化することもできる。しかし，
- 公開鍵で暗号化した文は，秘密鍵でしか復号化できない。
- 秘密鍵で暗号化した文は，公開鍵でしか復号化できない。
- 公開鍵と暗号化アルゴリズムを知っていても，その情報から (短い時間では) 秘密鍵を知ることはできない。

というのが，公開鍵暗号の原理である。このアイデアは一見単純に見えるが，ネットワーク上の暗号化通信を行う上での困難を一挙に解消する，画期的なものである。具体的に見てゆこう。

Abel と Briskorn がネットワークを通して通信を行う，という状況を考える。Abel の公開鍵を P_A, 秘密鍵を S_A とする。また， Briskorn の公開鍵を P_B, 秘密鍵を S_B とする。

(1) Abel が Briskorn に秘密メッセージ M を送りたいとする。

- Abel は Briskorn の公開鍵 P_B を使いメッセージ M を暗号化し，$P_B(M)$ として，ネットワークを通じて Briskorn に送る。
- このメッセージ $P_B(M)$ は，Briskorn の秘密鍵 S_B でしか復号化できないが，その秘密鍵 S_B を持っているのは Briskorn だけなので，Briskorn 以外の者がこの暗号化されたメッセージを入手しても，復号化できない。
- なおこの場合，Briskorn の公開鍵 P_B は一般に公開されているので，この暗号化されたメッセージの差出人が Abel となっていたとしても，それを書いたのが本当に Abel なのか？ という点については，確実な保障はない。

(2) 電子署名が可能となる。

- 証明書や申請書，借用書など，公式文書においては，それを書いた者が本当にその人物本人であることを証明したい場合がある。
- Abel は Abel 自身の秘密鍵 S_A を使い文書 M を暗号化し，$S_A(M)$ として，ネットワークを通じて Briskorn に送る。
- この暗号文 $S_A(M)$ は，Abel の公開鍵 P_A によって復号化でき，この鍵は公開されているので，これを入手した者はだれでもこれを復号化できる。
- これが Abel の公開鍵 P_A で復号化できたということは，それが Abel の秘密鍵 S_A で暗号化されたことを意味する。Abel の秘密鍵を持っているのは Abel だけなので，この文書を作成したのは Abel 本人であることが証明されたことになる。

さて，この公開鍵暗号のアイデアは，具体的にどのような方法で可能になるのだろうか？ 特に，

- 暗号化のアルゴリズムと公開鍵を知っている者が，その秘密鍵を計算できないようなシステムとはどのようなものか？

一般に，暗号化のアルゴリズムそれ自体を秘密にすることはできない。特にネットワーク上で使われるものは，ソフトウエアとして多くのコンピュータ・システムに実装されるので，暗号化の方法そのものは，完全に公開されていると考えなければならない。公開鍵を知った者は，当然その暗号化のアルゴリズムも知っており，それを解析することにより，それに対応した秘密鍵を計算することが出来たとしたら，この暗号化システムは全く役に立たない，ということになる。暗号化の方法と公開鍵を知っていても，その秘密鍵を計算できないようなシステムとはどのようなものか？

Diffie と Hellman は，公開鍵暗号の基本原理は考え出したのだが，それを実現するための具体的な方法は提示できなかった。

1978 年，MIT の Ron Rivest, Adi Shamir, Len Adleman の 3 人が，大きな素数の積を利用することにより，公開鍵暗号を実現する方法を見出した。この方法は，彼らの頭文字をとって，**RSA 暗号** と呼ばれている。(彼らはこれの特許を取ったが，それは 2000 年 9 月で切れている。)

演習問題 2.1

(1) Abel は Briskorn に，公開鍵暗号を利用し，ネットワークを通じて秘密のメッセージを送りたいとする。ただし，ネットワーク上で送られるデータは，常に盗聴者に見られる可能性がある。

次の条件 (a)〜(c) が全て満たされるようにするには，公開鍵暗号を利用して，どのような方法でメッセージを送ればよいか？

(a) Abel が Briskorn に送ったメッセージは暗号化されており，Briskorn 以外の人間は解読できない。

(b) Briskorn は，受け取ったメッセージが確実に Abel が書いたものであり，第 3 者が途中で改ざんしたものではないことを確認できる。

(c) このメッセージを送る過程でそのデータを盗聴した者がいたとしても，その内容を知ることはできない。

注： Abel の公開鍵を P_A，秘密鍵を S_A，Briskorn の公開鍵を P_B，秘密鍵を S_B とする。また，Abel が送るメッセージの平文を T とし，それを，鍵 S_A や P_B などによって暗号化して出来る暗号文を $S_A(T)$, $P_B(T)$ などという記号で表すこと。

(2)　A 国と B 国は長年紛争状態にあったが，C 国の秘密調停により和平交渉を行うことになった。A 国と B 国は，この交渉を行うにあたって，多くの秘密文書を通信経路を通してやり取りする必要があるが，これはあくまで秘密交渉の段階であり，A 国，B 国，C 国の交渉担当者以外の者に情報が漏れることを避けなければならない。

A 国から B 国へと秘密文書を送る場合，次の条件 (a)〜(c) が全て満たされるようにするには，公開鍵暗号を利用して，どのような方法で文書のやり取りを行えば良いか？

(a) B 国は，受け取ったメッセージが確実に A 国が作成したものであり，C 国を含めた第 3 者が途中で改ざんした可能性はないことを確認できる。

(b) C 国は，この交渉の過程を把握する必要がある。C 国は，A 国が B 国に送ったメッセージの内容を知る必要があり，さらに，その内容が確実に A 国が B 国に送ったものであることを確認できる。すなわち，A 国が実際に B 国へ送ったものと異なるものを C 国へ送ったり，B 国が実際に A 国から受け取ったものと異なるものを C 国へ送ったり，あるいは，第 3 者が A 国や B 国の名をかたって，A 国から B 国への文書であると偽って C 国へと文書を送ったりすることができないようにする。

(c) これらの文書のやり取りの中で，そのデータを盗聴した者がいたとしても，その内容を知ることはできない。

注 1： ただし C 国は，A 国と B 国の担当者が C 国に無断で勝手にやり取りする文書については，特に確認する方法はないものとする。上の (a)〜(c) は，あくまで A 国が B 国へと文書を送ったという申告があった時に，満たされなければならない条件である。

注 2： A 国の公開鍵を P_A，秘密鍵を S_A，B 国の公開鍵を P_B，秘密鍵を S_B，C 国の公開鍵を P_C，秘密鍵を S_C とする。A 国が B 国へ送ろうとする文書の平文を T とし，それを，鍵 S_A や P_B などによって暗号化して出来る暗号文を $S_A(T)$, $P_B(T)$ などという記号で表すこと。

(3)　(2) の A 国と B 国との和平交渉において，A 国は，C 国によって承認された文書を B 国へと送る必要がある場合がある。

次の条件 (a)〜(d) が全て満たされるようにするには，公開鍵暗号を利用して，どのような方法で文書のやり取りを行えば良いか？

(a) B 国は，受け取ったメッセージが確実にA国が作成したものであり，C 国を含めた第 3 者が途中で改ざんした可能性はないことを確認できる。

(b) A 国が B 国へと送る文書は，C 国が一度目を通したものであることを B 国が確認できる。

(c) C 国は，A 国が作成し，C 国が一度目を通した文書が，A 国自身や第 3 者によって改ざんされることなく B 国へと送られたことを確認できる。

(d) これらの文書のやり取りの中で，そのデータを盗聴した者がいたとしても，その内容を知ることはできない。

注： (2) の注 2 と同じ記号を使用すること。

2.4 群と公開鍵暗号

具体的な公開鍵暗号は 4 章以降で説明するが，ここでは一般的に，知られている公開鍵暗号が群の言葉で定式化されることに関して述べておく。

G をある種のタイプの有限群とする。E と D を自然数とする。ただし，G の任意の元 g に対し $\left(g^E\right)^D = g$ が成立するとする。このとき次の様な問題を考える。

離散対数問題 ： E と g^E が与えられたとき g を求めよ。

今群 G に対しては離散対数問題に答えることが**困難**であると仮定する。「困難である」ことの定義はデータの長さに関して多項式時間でそれを解くアルゴリズムが存在しない「と思われる」こととする。

このとき Abel はある方法で G と E, D を決定する。そして，G と E を公開し，D を秘密にする。自分に連絡する人に対し次のように暗号化することを要請する。

アルファベットの列または文章からなる集合 $\mathcal{T}$ と全単射である写像 $f : \mathcal{T} \longrightarrow G$ の存在は仮定する。

Briskorn が Abel に文章 T を送りたいとする。$g = f(T)$ を求め，Abel が公開している E を用いて $h = g^E$ を計算する。$T_1 = f^{-1}(h)$ を求め，T_1 を Abel に送る。

Cauchy がこれを盗聴したとする。Cauchy は内容が T_1 であることから，f で変換して h を得る。Cauchy は h はある元 g の E 乗であること，即ち $h = g^E$ であることは知っている。また Abel が公開しているので E の値も知っている。しかし離散対数問題の困難さから g を得ることはできない。

Abel は秘密 D を知っているので $h = g^D$ を得た場合 $h^E = \left(g^D\right)^E = g$ より，文 $T = f^{-1}(g)$ を得ることができる。

この様な G が存在するか，具体的に計算可能な等の問題は後回しにして，ここでは，離散対数問題の解決が困難な群のタイプを見つけられたとして，ここで述べた方法は公開鍵暗号の条件を満たすことを確認しておこう。公開鍵暗号は以下の条件を満たす必要があった。

- 平文は，公開鍵で暗号化することもできるし，秘密鍵で暗号化することもできる。しかし，
- 公開鍵で暗号化した文は，秘密鍵でしか復号化できない。
- 秘密鍵で暗号化した文は，公開鍵でしか復号化できない。
- 公開鍵と暗号化アルゴリズムを知っていても，その情報から (短い時間では) 秘密鍵を知ることはできない。

離散対数問題が困難であることから最後の条件は満たされる。すでに見たように公開鍵で暗号化した文は秘密鍵でしか復号化できない。

秘密鍵による暗号化は公開鍵による暗号化と全く同じであるが，この鍵を知っているのは Abel だけである。文 T に対応する $g = f(T)$ を E 乗し $h = g^D$ を得る。公開鍵 E を知らない人には h から g を求める問題は同じく離散対数問題となる。よって公開鍵 E を知らない人間には復号化できないことになる。