暗号の数理要綱 #1

0 Introduction

この節ではイントロとして暗号に関して簡単に概説しておこう。

古代ローマでカエサルが用いたことで有名なのが，カエサル暗号 (シーザー暗号) である。換字式暗号の最も簡単なタイプである。カエサルはアルファベットを 3 文字ずらすことで文書を暗号化した。

カエサル暗号を例にとり暗号について簡単に説明しよう。暗号の話では Alice，Bob，Catharine という名前がよく登場するが，ここでは Abel，Briskorn，Cauchy の 3 人とする。

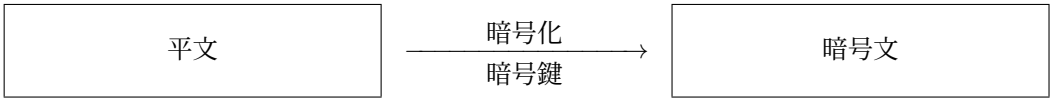
Abel(アルファベットの A で始まる名前) が Briskorn(B で始まる名前) に何らかの情報を伝えたい状況を想定する。ただし Cauchy(C で始まる名前) がその情報を知りたがっていて，途中で盗み見る可能性があるとしよう。Cauchy が盗み見ても分からないように Abel と Briskorn はカエサル暗号を用いることを予め打ち合わせしたとする。カエサル暗号は文字を 3 文字ずらすが，Abel と Briskorn は -3 文字ずらすことを打ち合わせたとしよう (この暗号もカエサル暗号と呼ばれる)。この方法で暗号化することを考える。

Abel が，例えば「meet at midnight」という文章を Briskorn に送りたいとする。a→x,b→y,c→z,$\cdots$ と変換することになる。文字の対応表を書くと下記のようになる。ここで暗号化の前と後を区別するため，暗号化後の文字を大文字で書いた。

```
abcdefghijklmnopqrstuvwxyz
XYZABCDEFGHIJKLMNOPQRSTUVW
```

これを用いて変換すると (この操作を暗号化という) 文章は「JBBQ XQ JFAKFDEQ」となる。Abel はこれを Briskorn に送る。Cauchy はこれを盗み見るが意味が分からない。Briskorn は受け取った文章「JBBQ XQ JFAKFDEQ」を対応表を使って変換する。この操作を復号化という。Briskorn は「meet at midnight」という文を得る。Abel は Cauchy に知られずに Briskorn に情報を送ることができた。めでたし，めでたし。

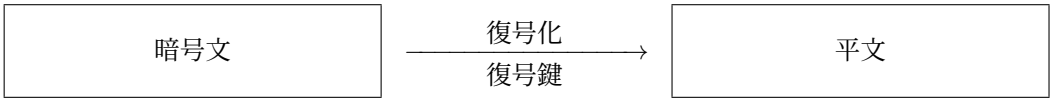
しかし，Cauchy が暗号文を見て考えたとしよう。「これはカエサル暗号かもしれない。」Cauchy は普通の 3 文字シフトで解読を試みる。「やってみよう，うーん意味が取れない。」ここであきらめるかもしれない。しかし 4 文字シフトを試みる。「うーん，うまくいかない。」ここであきらめるかもしれない。しかし Cauchy が次々とシフトを増やしていったとしよう。あきらめなければ 23 シフトで元の文章を得ることができる。このような作業を解読と呼ぶ。



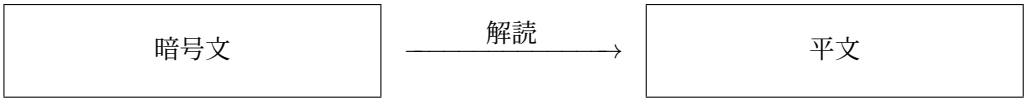
ここで暗号化，復号化について少し一般的に説明しておこう。暗号化とは通常の文書 (平文と呼ばれる) を変換して，変換について情報をもっていない人間には理解しにくい文書 (暗号文と呼ばれる) に変換することをいう。ここでアルゴリズムと暗号鍵を分けておく[(1)]。一般にアルファベット n 文字シフトさせる暗号はカエサル暗号と呼ばれる。今の場合カエサル暗号というアルゴリズ

[(1)] アルゴリズムと鍵の切り分けは絶対的なものではないが，考察に便利なので通常行われている。一般に「鍵は秘密にできるがアルゴリズムは秘密にできない」というのが暗号解読における「鉄則」になっている。

ムを採用した。暗号鍵にあたるのが -3 である。アルゴリズム + 鍵で -3 文字シフトさせるということが分かる。



暗号文を鍵 (復号化の鍵を復号鍵と呼ぶ) を用いてもとの文章に変換する操作を復号化と呼ぶ。今の場合復号化のアルゴリズムは暗号化と同じで，復号鍵は 3 である。一般に復号化のアルゴリズムが暗号化のアルゴリズムと同じということはない。



暗号文が与えられたとき，暗号鍵および復号鍵を知らないという条件のもとで，暗号文を平文にもどす操作を解読と呼ぶ。解読がしやすい暗号を「弱い暗号」，解読しずらい暗号を「強い暗号」という[(2)]。

カエサル暗号は 25 通りしかないので，カエサル暗号で暗号化されていると分かれば簡単に復号化できる非常に弱い暗号である。しかし，アルゴリズムを少し変えると，少し強い暗号となる。この強力化されたカエサル暗号はキーワード (鍵語) またはキーフレーズ (鍵句) を用いる。例えばキーフレーズとして KOUNO MASAHARU を採用しよう。最初にキーフレーズから重複する文字を消去する。キーフレーズとして「KOUNMASHR」を得る。これを最初に書き，そこに含まれないアルファベットを今書いた最後の文字 (今の場合 R) の次から順に書いていく。対応表は次のようになる。

```
abcdefghijklmnopqrstuvwxyz
KOUNMASHRTVWXYZBCDEFGIJLPQ
```

前の文章を暗号化すると次のようになる。

```
meet at midnight
XMMF KF XRNYRSHF
```

この暗号は解読するのが難しそうに見えるが解読する方法は実は存在する。一般にアルファベット換字暗号を定式化しよう。$\mathcal{A} = \{ a, b, c, \ldots, x, y, z \}$，$\mathcal{B} = \{ A, B, C, \ldots, X, Y, Z \}$ とする。暗号化とは $\mathcal{A}$ から $\mathcal{B}$ への一対一写像 f を指定し，それにより各文字を変換することと考えることができる。上の例でいうと写像 f は $f(a) = K, f(b) = O, f(c) = U, \ldots$ となっている。復号化とは f の逆写像 f^{-1} を考え，それにより各文字を逆変換することと考えることができる。このように与えられる暗号をアルファベット換字式暗号と呼ぶ。

アルファベット換字式暗号はそれほど強くはない。どのような f を指定しようとも f は一対一という性質を持っているので，1 つの文字には 1 つの文字が対応する。各言語で文字の出現頻度は調べられており，それをもとに推定することが考えられる。英語の場合を考えると出現頻度が一番大きいのが「e」である。暗号文中に表れる文字で一番出現頻度が大きい文字が「e」に対応すると考えて考察を進めることができる。勿論短い文章では頻度分析からはずれることもある。暗号解読においては理論的にはいくらでも長い暗号文が得られることを仮定して解読を試みるので今の場合

[(2)] これは「文学的」定義で厳密な定義では勿論ない

このことは考察外としよう。長いテキストの場合一般的には標準的分布になることが期待される。ただしこのことはいつでも正しいとは限らない。1969 年フランスの作家ジョルジュ・ペレックが 200 ページの小説『消失』を発表したが，この作品には「e」が一文字も含まれていなかった。これをイギリスの小説家兼評論家ギルバート・アデアが「e」を 1 文字も使わずに英訳した。そのような特別な場合もあるが，一般的には標準的な頻度分布に従うとしてよいだろう。暗号文解読はレポート課題とするので興味のある人はチャレンジしてみて下さい。

暗号は軍事を中心として歴史的に用いられていたが，運用上一番の問題は鍵配送問題であった。暗号化し復号化するためには鍵を知る必要がある。Alice と Bob が離れた場所にいる場合，Abel が鍵を決定したとして，それをどのように Briskorn に伝えるかが問題になる。電話などで伝えた場合 Cauchy が盗聴しているかもしれない。

Abel が Briskorn に会って直接鍵を手渡す (教える) という方法が考えられる。また Abel の信頼できる人間に Briskorn に会って鍵を手渡す方法も考えられる。実際長い間鍵配送は後者の信頼できる人間が直接渡すという方法で行われてきた。近代のほとんどの軍隊はそのようなことのために専門の組織を持っていたし，第 2 次世界大戦後の多国籍企業もそのような人間を雇っていた。そのためにはコストがかかり個人で利用するということは考えられなかった。しかしディフィー，ヘルマン，マークルの 3 人は 1976 年 6 月の全米コンピュータ会議で,「鍵配送問題は解決可能である」ことを公表し，集まった暗号専門家を驚愕させた。

きちんとした説明は後でするが，ここではたとえ話をしておく。Abel が Briskorn にある文書を秘密裏に届けたいとする。Abel はその文書を鍵のかかったトランクに入れて Briskorn に送る。受け取った Bob はトランクに自分の鍵を更につけて Abel に送り返す。この段階でトランクには鍵は 2 つついている。送り返されたトランクを Abel は自分の鍵を用いて開ける。この段階でトランクについている鍵は Briskorn のものだけになる。このトランクを Abel は Briskorn に送る。Briskorn は自分の鍵でトランクを開けて Abel の手紙を読む。どの段階でも鍵がかかっているので，鍵を破れなければ，他人は文書を読むことができない。

ただしこのたとえ話を実際に暗号で実装するにはまだ困難が残っている。暗号の話に直すと上のことは次のようなことに対応する；Alice が自分の鍵を用いて暗号化した暗号文を送る → Bob はその暗号文を自分の鍵を用いて更に暗号化して送り返す → Alice はその文書を自分の鍵で復号化して Bob に送る → Bob は自分の鍵でその文書を復号化する。

この方法では一般に元の平文を得ることはできない。暗号化・復号化は順序が問題で，Alice の暗号化・復号化を暗号化 A・復号化 A と書き，Bob の暗号化・復号化を暗号化 B・復号化 B とすると

$$\text{暗号化 A} \longrightarrow \text{暗号化 B} \longrightarrow \text{復号化 B} \longrightarrow \text{復号化 A}$$

の順なら元の平文が得られるが,

$$\text{暗号化 A} \longrightarrow \text{暗号化 B} \longrightarrow \text{復号化 A} \longrightarrow \text{復号化 B}$$

では一般には元の平文は得られない。この順序で暗号化・復号化を行って元の平文が得られるような強い暗号が必要になる。

最後に非対称鍵暗号・公開鍵暗号にふれてイントロを終わろう。1976 年以前は暗号といえば**共通鍵暗号** (*common key cryptosystem*) であった。当時は「共通鍵暗号」という概念もなく暗号と言えば (今でいう) 共通鍵暗号をさしていた。共通鍵暗号とは復号鍵が暗号化に用いる鍵と同一，または，

暗号化鍵から容易に導出可能である暗号方式である。**対称鍵暗号** (*symmetric key cryptosystem*) とも呼ばれる。また鍵を秘密にする必要があることから**秘密鍵暗号** (*secret key cryptosystem*) とも呼ばれた。それに対し**非対称鍵暗号** (*non-symmetric key cryptosystem*) とは秘密の知識なしには暗号鍵から容易に導出が不可能な復号鍵をもつような暗号，またはその逆に，復号鍵から容易に導出が不可能な暗号鍵をもつような暗号である。**公開鍵暗号** (*public key cryptosystem*) とははこの非対称暗号の「一方の鍵の公開可能性」に着目した命名と考えられる。

非対称暗号が存在するかどうかというのは重要な問題だが，今は存在を仮定して話を進める。Abel は非対称暗号で自分の暗号鍵・復号鍵を決定し，復号鍵は秘密にし暗号鍵を公開するとする。そして自分に秘密裏に連絡をとりたい人はその暗号鍵で暗号化して送るように要請をする。Briskorn は Abel に秘密裏に連絡をとりたいので，文書を Abel の暗号鍵で暗号化して送る。Cauchy は Abel の暗号鍵を知っているが，盗聴しても復号鍵を知らないため内容を知ることができない。

Cauchy が盗聴ではなく改竄を試みている状況を考える。Abel は自分の別の暗号鍵・復号鍵を決定し，暗号鍵は秘密にし復号鍵を公開し，自分からの連絡はすべてこの鍵で暗号化して送ると公表する。そして Briskorn に送る文書を自分の暗号鍵で暗号化して送る。Cauchy はその文書を途中で盗むことができたとする。Cauchy は暗号文を復号化して元の文書を読むことはできる。しかし改竄した場合，その文書を暗号化して Briskorn に送る必要がある。暗号化の方法は知らないので改竄することはできない。Briskorn に暗号化された文書が届いたとき，Abel の復号鍵で復号できれば，その文書は Abel からのものに間違いないと考えてよいことになる[(3)]。

1976 年にディフィー，ヘルマンがこの「非対称鍵暗号・公開鍵暗号」の概念を提出したとき，自身もそのような暗号の存在に関し情報を持っていなかった。ディフィー，ヘルマンがこのアイディアを公開した当初は楽観ムードにあふれていて数ヶ月でそのような暗号が見つかるという雰囲気で探索は行われた。しかし，なかなか見つからないので「そのようなものはないのでは」という声も出始めたとき，RAS 暗号が登場する。1977 年にロナルド・リヴェスト，アディ・シャミア，レナード・アルドマンの 3 人が非対称暗号，現在 RSA 暗号と呼ばれる暗号を発表し現在にいたる。これに関して理解を深めることがこの講義の目的の 1 つである。

公式の歴史はここまでであるが「非公式」の歴史がある。彼ら以前に鍵配送問題・非対称暗号・RSA 暗号のアイディアを得た人達がいる。イギリス政府の最高機密機関の所属だったために公開されることはなかったが，ジェイムズ・エリスは 1969 年に鍵配送問題の解決と非対称暗号 (エリスの呼び方だと非秘密暗号) のアイディアを得ていたし，クリフォード・コックスは RSA 暗号のアイディアを 1973 年に得ていた。この話はサイモン・シン『暗号解読』(新潮社；文庫化されたようです) に詳しい。この話も含めこの本は非常に面白いのでお勧めです。

[(3)] 代表的な公開鍵暗号である RSA 暗号は鍵が暗号化にも復号化にも使える。即ち鍵 A と鍵 B を生成し，鍵 A を公開し鍵 B を秘密にしたとする。鍵 A で暗号化した暗号文は鍵 B で復号化できるし，鍵 B で暗号化した暗号文は鍵 A で復号化できる。盗聴防止のためには Bob は公開鍵 A を用いて暗号化して送ればよい。改竄防止のために Abel は自分の秘密鍵 B を用いて暗号化して Briskorn に送ればよい。