国際科学科1年 KGS研究Ⅰ:数学編

暗号解読

1 ねらい

今日のKGS研究Ⅰの授業では,『暗号作成→暗号解読(復号)』 を実際に取り組みながら,その奥に隠された数学的要素を学習します.

コンピュータでは文字は全て2進数の数値に置き換えられるので「文字」と「数値」は同じで,ディスプレー画面に表示するときだけ異なります.今では,あらゆる処理をコンピュータがするようになり,暗号も「文字」から「数値」へと変化しています.個人のプライバシー保護,情報の改ざん防止,電子証明書や電子現金などの信用証明,なりすまし防止,インターネットでの買い物,銀行口座の手続きなど,あらゆるシステムを根本で成り立たせているのが『暗号』です.

この授業を通して暗号に隠された数学的要素を学習し,さらに興味を持った人は,今後の課題研究につなげてください.では,『暗号解読』スタートです!

2 「公開鍵暗号」の誕生

モリくんは,今,インターネットで知り合ったカトウくんにメッセージを送ろうとしています.メッセージの内容は誰にも知られたくありません.
そこでモリくんは,メールの文章を暗号化して暗号文を作成しました.

問1 モリくん以外の誰にも復号されない暗号の手順を考えてみよう.

ここからは,暗号化や復号化の手順を「鍵」というワードを用いて表します。

では,モリくんは暗号文と鍵の両方をカトウくんに送ればOKでしょうか?いいえ,暗号文と鍵の両方を送ってしまったら,その途中で誰かに見られてしまう危険があります.モリくんは暗号文を復号する「鍵」を送ることができないのです.

そこで誕生したのが「公開鍵暗号」という方法です.公開鍵暗号では,鍵を2つ用意します.暗号化するための鍵(「公開鍵」といいます)と,復号するための鍵(「秘密鍵」といいます)の2つです.

まず,カトウくんは公開鍵と秘密鍵のペアを作ります.秘密鍵は大事に閉まっておきます.公開鍵はモリくんに送って,「僕にメールを送るなら,この鍵で暗号化してね」と伝えておきます.

モリくんはこの鍵でメールの文章を暗号化して暗号文を作成します.この暗号文をカトウくんに送ればOKです.暗号文を受け取ったカトウくんは,自分の秘密鍵を使って暗号文を復号し,元のメッセージを読むことができます.

途中で誰かに見られてしまったら?・・・,大丈夫です.暗号文を見ても内容はわかりませんし,公開鍵を知っても,それを使って暗号文を元に戻すことはできないからです.

⇒ 誰かが公開鍵や暗号文から秘密鍵を推測できてしまったら,元のメッセージも読まれてしまいます.しかし,そこには絶対に推測不可能と言える**ある数学的要素**があり,安全性を保証しているのです.

3 RSA暗号をやってみよう

公開鍵暗号の代表的な方法が「RSA暗号」と呼ばれるものです.今日は,RSA暗号について学習し,実際に暗号化・復号を試みてもらいます!

コンピュータでは文字と数値は同じです.一般的にはＡＳＣＩＩ(アスキー)コードを用いて文字を数値にするが,今日は下のオリジナル文字コードを用いて文字と数値を対応することにしましょう.

≪オリジナル文字コード≫

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
P	Q	R	S	T	U	V	W	X	Y	Z	!	“	#	$
31	32	33												
%	&	‘												

例1 上のオリジナル文字コードを用いて,「ANGOU」を数値にすると,(1, 14, 7, 15, 21)となる.

問2 上のオリジナル文字コードを用いて,「KIBOU」を数値にせよ.また,(5, 19, 16, 15, 9, 18)を文字に直せ.

(1) 暗号化してみよう

RSA暗号では，元の文も，暗号文も，鍵もすべて数値です．数Eと数Nを用いて，RSAの暗号化は次の合同式で表現することができます．

(RSAの暗号化)

数Eと数Nがわかれば暗号化することができます．EとNという2つの数を一組にした(E, N)が［　　］です．

例2　文字「N」を暗号化する．ただし，公開鍵(7, 33)とする．

オリジナル文字コードより，文字「N」を数値にすると　N→14　となる．

この14に公開鍵(7, 33)を使って暗号化すると

$$(\text{元の文})^{E} \pmod{N} \equiv 14^{7} \pmod{33} \equiv 105413504 \pmod{33} \equiv 20 \pmod{33}$$

オリジナル文字コードより，数値「20」を文字にすると　20→T　となる．したがって，文字「N」を暗号化すると文字「T」である．

問3　文字「 C 」を暗号化せよ．ただし，公開鍵(7, 33)とする．

(2) 復号してみよう

問4　公開鍵(7, 33)で暗号化された，文字「 I 」を復号せよ．

盗聴者が，公開鍵の「(7, 33)」を手に入れたとしても，「 $\blacksquare^{7} \equiv 20 \pmod{33}$ 」の式から■に入る数字を求めることはできないのでしょうか．

もしも mod 33 がなく，「 $\blacksquare^{7} = 20$ 」という式であれば，暗号化された文字から元の文字を求めることはそれほど難しくありません．(これは対数と呼ばれるものを求める問題に帰着されます)．けれど，　mod 33　がついていると非常に困難な問題になってしまいます．

復号も暗号化同様，数Dと数Nを用いて，次の合同式で表現することができます．ただし，数Nは暗号化で用いた数字と同じものを使います．

(RSAの復号)

数Dと数Nがわかれば復号することができます．DとNという2つの数を一組にした(D, N)が［　　］です．

例3　文字「T」を復号する．ただし，秘密鍵(3, 33)とする．オリジナル文字コードより，文字「T」を数値にすると　T→20　となる．

この20に秘密鍵(3, 33)を使って復号すると

$$(\text{暗号文})^{D} \pmod{N} \equiv 20^{3} \pmod{33} \equiv 14 \pmod{33}$$

オリジナル文字コードより，数値「14」を文字にすると　14→N　となる．したがって，文字「T」を復号すると文字「N」である．

問5　モリくんから次のメールが届きました．

「 カトウくんへ：冷蔵庫のプリンを食べたのは【 P A V O P 】だよ 」

カトウくんはモリくんに公開鍵(7, 33)を伝えてあり，モリくんはこの公開鍵で暗号化した．カトウくんが持っている秘密鍵は(3, 33)であるとき，カトウくんの代わりに暗号を解読せよ．

(3) 公開鍵(E, N), 秘密鍵(D, N)を求めてみよう

(1)(2)で出てきたE, D, Nはどんな数でもいいわけではありません. 作成手順は次のようになります.

① Nを求める ②Lを求める(Lは鍵の生成のときだけ登場する数です) ③Eを求める ④Dを求める

大きな素数を2つ用意します. 2つの素数をp, qとすると, Nは [　　] という式で表現します.

② Lを求める

Lは暗号化にも復号にも登場しない, 鍵を作るときだけ現れる数です.

①で出てきた素数p, qを使って, Lはp－1とq－1の [　　] である数です.

③ Eを求める

Eを求めるには, 次の2つの条件を満たすような数を探してきます.

その1 1<E<L

その2 EとLは [　　]

④ Dを求める

Dは, 次の2つの条件を満たすように, Eから計算して求めます.

その1 1<D<L

その2 EとDは [　　] という関係式を満たす

※大ざっぱな話をすると, その2の関係式は「暗号文を復号すると元の文章に戻る」ということを意味しています.

問4 具体的に公開鍵(E, N)・秘密鍵(D, N)を生成してみよ. あまり大きな数を使うと計算が大変なので, p＝3, q＝11とする.

4 RSA暗号の安全性

例2と例3の結果を見比べてもわかる通り，公開鍵を使って暗号化した文字は，秘密鍵を使ってきちんと復号できます．
また，問4において，公開鍵で復号することは難しいことも確認しました。
さらに，実際には大きな素数を使ってNを生成するため， mod N がついた式では，より求めるのが困難な問題となってしまうのです．

しかし，秘密鍵がばれてしまえば，盗聴者はそれを使って元の文を読むことができます．公開鍵から秘密鍵を求めることはできるのでしょうか？

問7　盗聴者は公開鍵(7，33)だけを知っているとします．公開鍵(7，33)から，秘密鍵(D，33)の数Dを求めることはできるか，考えてみよう．

RSA暗号の安全性は，大きな数Nを［　　］することが困難であるために保証されている．

補足　1991年以降 RSA Security 社は，色々な桁数の「素数と素数の積」の素因数分解問題を出題するRSA Factoring Challengeというコンテストを実施しています(コンテスト自体は2007年まで)．現在の最高記録は，2009年にNTTがスイス，ドイツ，フランス，オランダの大学および研究機関と共同研究で成功した，768ビット(10進 232桁)の合成数に対しての素因数分解です．

【その時の分解がこちら】

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413 （232桁）
＝
3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9（116桁・素数）
×
3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7（116桁・素数）

一般的なCPUを搭載したコンピュータなら，約1500年かけたのと同程度の計算量を要しました．実際には，2007年から分解を始め，PCクラスターなど300台程度のコンピュータを用いて，約3年かかったといいます．

研究2　素数は無限に存在することが知られています．素数の性質などについて研究してみよう！

研究3　公開鍵暗号が発明される以前，人類は様々な工夫をして暗号化を試みてきました．「対称暗号(共通鍵暗号)」などについて研究してみよう！

(　　)番 氏名(　　)