暗号数理学者釜賀一夫のこと

福富節男

振り返っての恐怖　始めから横道へゆく。１９４５年８月１５日、降伏宣言の昭和天皇の声の録音盤がまわって、彼の声を聞いた日である。その放送がまだされていない午前中に、学生たちの前で私は学生たちに、「日本は負けました。降伏の使節がフィリピンに向ってゆくでしょう。負けたにしても貴方たちの働きは、米軍が来て知っても驚くでしょう」と話した。後半は動員されていた学生たちへの、慰めの発言である。「七生報国」なんて言葉は私の「言葉集」にはなかった。その他にも言った言葉を記憶していた当時の学生が何十年かの後になって語ったり、書いたりしている。学生というのは東京文理大（現筑波大の前身）数学科の学生が４人、東京女子大の英語科の３人、数学科１年生３０人で、彼等に手伝ってもらって、暗号の乱数とか、ストリップ式暗号のシミュレーションなどをしていた。そこは参謀本部陸軍特種情報部の特別研究班といった。将校は私一人、下士官が一人であって、作業する人びとは動員の学生たちであった。ここを特別研究班と名づけて、研究をやってもらう人を東京に残そうとしたのだと、ずっと後になって釜賀一夫さんが話してくれたのである。

なぜ日本の敗北をさきばしって言ったのか、もし降伏が二、三ヶ月でも遅れたら、憲兵に引っ張られたかも知れぬというのが、何十年もたってからの、想像上の恐怖になった。五年ほど前にその恐怖から解放されることになった。

国際集会「数学と戦争」にレポートを出すことになった。鹿野忠良さんの勧めである。私の原稿は鹿野さんが直ちにフランス語に訳してコンファレンス主催者に送ってくださった。鹿野さんは、ベトナム問題に関する数学者懇談会と日本の米暗号解読研究のこと、弥永先生が自身の戦争協力について自己批判をしたことを書くとよいといった。暗号解読という６０年も前の仕事を書くために、かつての上官の釜賀一夫にしばらくぶりに会うことにした。１９４５年８月１４日夜、釜賀さんは「下宿で、暗号関係の書類の焼却を手伝ってもらった」という。私が「戦争のことは忘れようとしていたので、憶えていません」いうと釜賀さんは苦笑した。そのことを聞いて思い出したのは、釜賀自身の計算のメモまで焼いたことである。これで私は回想的恐怖から解放された。後述の陸軍中央特種情報部でも、あらゆるものを焼却した。フィリピンから捕ってきたパンチカード式高速リレー電気計算機も分解し、隅田川に投棄した。これは有名な機械らしく、後に米軍の知るところとなり、旧陸軍は川浚いを命令された。当時は日本では情報の保存や公開に関する、関心や知識は乏しかったと思うが、当時の資料をすべて焼却したのは残念なことである。

陸軍中央特種情報部・参謀本部　私が１９４２年軍隊に召集され、４４年に樺太の砲兵連隊から参謀本部の陸軍中央特種情報部（これが正式名称で外部には陸軍中央通信調査部と言っていた）に転属させられたとき、釜賀一夫は当時陸軍大尉（後に少佐）で、参謀本部の暗号作成の部署から情報部にときたま暗号解読の指導に来ていた。私の軍隊生活で接した上官の中で尊敬できた、

たった二人の人物の一人であった。情報部の数学関係者では後に広島大の数理統計学の教授をする山本純恭が私より一期上にいた。

私たちはストリップ式暗号（図１）と機械暗号（図２）の二種類の解読に従事した。解読とは暗号の鍵をもたないで、原文(平文―ひらぶん―という)を知ることであり、鍵とコードブックに照らして原文を知るのは翻訳といった。部隊のいわゆる暗号兵はコードブックをもちいて、自軍の原文の暗号化をするか、自軍の暗号文を翻訳するのである。

この機械暗号機のもとはスウェーデン製の商業暗号機でクリプトテクニークといい、同国でハゲリン機といっている。ハゲリンはクリプトテクニークを開発し、生産する会社をたてた人である。米軍がクリプトテクニークを改造し、それをＭ２０９と呼んでいたことを戦後に知った。

釜賀一夫は一人の数学者を参謀本部に採用した。私より一年下の山本幸一君で、末綱恕一教授のところで解析数論と代数を学んでいた。参謀本部の暗号作成の部署にいてラテン方陣、オイラー方陣の応用を研究をしていた。戦後に Combinatorics の専門家となり、九大、Wisconsin 大、金沢大、東京女子大などの教員（助手、教授）をした。

釜賀は参謀本部で暗号作成に従事し、後述の「字差の理論」を生み出した。彼は無限乱数方式の暗号を確立した。無限乱数作成には０００００から９９９９９までを書いたカードを箱に入れて、振り混ぜて、一枚ずつ取り出して数字を記録してはカードをもとの箱にもどすという方法をとったらしいが、私はその実際の作業をみていない。その作業をしていた人は殆ど生存していないだろう。

釜賀一夫は１９１７（大正６）年１月１日、熊本市字土郡（現宇土市）にうまれた。陸軍士官学校卒業（５０期）、佐世保重砲兵連隊の砲兵少尉のとき暗号教育を受け、その成績がはなはだ優秀であったので、陸軍通信学校で本格的に暗号教育をうけることになり、ついで参謀本部の暗号班に抜てきされた。ノモンハン事件に従軍した。その頃は無線通信の通信機材もわるく、通信手も上手でなかったので、非常に誤りが多く、まともな姿で電報が来ず、判読に苦労した。私物暗号などを使う連中もいたなどと述懐している。これが釜賀をして「字差の理論」、いまでいえば Hamminng の符号理論に相当するものの開発にむかわせたのだろう。

釜賀は本務の合間に特情部にきて、私たちにストリップ式と Ｍ２０９の手ほどきをした。クリプトテクニークでは原文（平文）の単語の切れ目に文字 X を使っていたが、米軍は X の代わりに Z を使っていることがわかった。これはこちらから語学関係の将校をマニラに派遣し、捕虜収容所で米軍捕虜の暗号兵から聞きだしたことである。そこで我われは Z 暗号と呼ぶことにした。米軍の機械はクリプトテクニークをどう改造したものなのかを推理し、的中させたのは山本幸一である。これはこの暗号の解読の上でもっとも大きなことである。ある一通の暗号文に対する英語当てはめに最初に成功したのは彦根高商出身で英語に練達の西岡勝彦であった。外見の鍵を暗号化して真の鍵を秘匿しているらしいので、私はそれを見つける方法に腐心した。どうやらうまく行ったと思った。また原文をいくつかに区切って、括弧で括り、括ったものを転置するらしいということになった。括弧をＰＲＮ（parenthesis の略記号）で表わしているらしいので、その位置を

見つけることは解読の手がかりになった。この‘ＰＲＮ’の位置をみつけることを、私たちはプルン作業と呼んでいた。

釜賀は陸軍の員外学生として１９４３(昭和１８)年東大理学部物理学科に入学する。同級には作曲家になる別宮貞雄がいる。数学科に行きたかったが陸軍は数学科への進学を認めず、物理学科へなら入学を認めた。「員外」とは陸軍の本務の定員外というほどの意味で、大学の側からみては委託学生とよばれた。

私との関係でいうと、釜賀は上官であり、ときには同僚のようでもあり、そして理学部の後輩ということになる。ちょっとＭ２０９の解読についての挿話を付け加えよう。中国戦線の衡陽（洞庭湖の南約２５０キロ）で墜落した米軍機のパイロットのポケットから、攻撃命令を（平文で）記した細いテープをみつけた。見つけた憲兵は、重要なものらしいと察し参謀本部に送ってきた。たまたまこの平文に対応する暗号文が傍受されていた。これがクリプトテクニーク機によるものではないかと考えるきっかけとなり、Z暗号の解読作業が始まる。

陸軍数学研究会（陸軍暗号学理研究会）　釜賀は大学の数学の教授らの協力を求める仕組みを作ろうと考えていた。陸軍は暗号使用上の秘密保持上の不安があるといって、外部の協力に反対であった。しかし当時の特情部長が責任を持つと言って、釜賀は１９４３(昭和１８)年から数学者の協力を求めることを始めることができた。陸軍科学学校―砲工学校の後身―の教官雀部峻三（東大数学科で吉田洋一と同期）の案内で、高木貞治のところに赴いた。高木は役に立たないでしょうと消極的であったが、話くらいは聞くといって、釜賀から暗号の講義を聴くことになった。これが翌年陸軍暗号学理研究会（外部に対しては陸軍数学研究会）に発展することになる。釜賀の大努力の結実である。これは木村洋の論文に詳しいから省こう。エピソードを挿入しよう。陸軍数学研究会委員の名簿にある幹事の金子昌雄中佐は参謀本部第三部通信課暗号班長であった。新しい暗号書を携行し、シベリア鉄道でモスクワに向ったが、途中酒好きの金子はウォッカを相客にしたたか飲まされ毒殺された（１９４５年４月２９日）。このようなことになると当然暗号書は盗写されたろうから、全面的に作り直さなければならない。釜賀は多忙になったはずだが、任務も部署も違うから、私は釜賀に経緯を聞くなどはしなかった。そのころ東行何輌、西行何輌というシベリア鉄道の運行状況が伝えられていて、部内回覧の文書の中で見た記憶があるが、それが金子中佐による電報であったか今は、断言する自信はない。

諏訪に東大数学科が疎開し、同時に上記の陸軍数学研究会も行なわれていた。ある時、半偶数のオイラー方陣が存在しないというEulerの予想を証明したという、Ｐ．Wernicke　の証明が話題になり、「おや、この証明は間違っている」と誰かが言ったが、「それが小平さんか河田さんのどちらかだったか忘れた。気になっているが、弥永先生に聞けないだろうか」と釜賀が語っていた。オイラー方陣を使って暗号作成をすることを、釜賀や山本幸一がやっていた。（後年$n \neq 2, 6$のときを除いて、すべての次数のオイラー方陣が存在することが示された。1960年の日本数学会機関紙「数学」11巻1号の雑報、同12巻2号の山本幸一の論説中に紹介されている）

字差の理論　これからがいわば本論である。１９４４年夏釜賀は「福富君これはどうかね？」といった。字差という言葉をきいたのは、それが初めてであった。それはある種の距離ですねとは返事したのだが、暗号作成の方の現場を知らず、関心もない私はそっけない返事をしてしまった

暗語（ベクトル）$\mathbf{x}=(x_1,x_2,\cdots,x_n)$, $\mathbf{y}=(y_1,y_2,\cdots,y_n)$の距離を

$$d(\mathbf{x},\ \mathbf{y})=\sum_{i=1}^{n}\delta(x_i,y_i)$$

で定義する。ここで　$\delta(x,\ y)=1\ (x\neq y)$, $\delta(x,\ y)=0\ (x=y)$。

これは現在Hamming距離と呼ばれるものである。これを字差と呼んだのは釜賀の上官の原　久中佐（４１期）であった。

暗語の集合（釜賀の用語では暗号群）C について、使用文字数をn，暗語を構成する記号数をgとする。nとしては２，３，４，…２６、gとしては　２，３，４，５などが通例である。暗語$\mathbf{x}$，$\mathbf{y}$の字差を考える。C　に属する任意の二つの暗語の字差の最小値がMのとき C は完全M字差であるという。

当時釜賀の得た定理は次のようなものである。

定理１（字差構造の定理）：　C が完全M字差 ⇔ 使用文字中任意の$M-1$文字を抹消した$g-(M-1)$記号の暗語集合は完全1字差となる

定理2（字差制限の定理）：使用文字数　n、記号数　g の完全M字差の暗語集合 C の暗語数(釜賀は暗語得数と呼んでいる)は $\leqq n^{g-M+1}$

定理3 ：n 個の文字を $0,1,\cdots,n-1$ とし　暗語成分を x_i と書くとき,

$$\sum_{i=1}^{g-1}x_i\equiv x_g\pmod{n}$$

関係をみたす、すべての暗語集合は完全2字差であり、その暗語の総数は n^{g-1}個である。

定理4：x_iは定理3 と同様とする。

$$x_1+x_2+\cdots x_{i-1}+x_{i+1}+\cdots+x_g\equiv x_i+k\pmod{n}$$

を満たす暗語の集合は完全2字差であり、その暗語の総数は n^{g-1} である。

これらを基礎に、字差に関する多くの定理が、彼の著『字差概論』に記されている。さらにラテン方陣、オイラー方陣を応用した暗号の構成と、得られる暗語集合の字差について多くのページを使って記している。またさらに釜賀は暗号強度と字差の関係、通信における誤字、脱字、冗字の検出についての字差の有効性を論じている。 さらに完全 2字差暗号における誤字の判読の要領などについて述べ、誤字の生起状況の実態に及んでいる。以上の理論を戦時中に釜賀は『字差概論』という著書にまとめたのである。

後年の著『基礎暗号学』には、より明瞭な次の定理が記されている。

定理5 (字差効果に関する定理): g 記号完全 M 字差暗語集合 C において 1暗語中 $M-1$ 以下の誤字は検出できる。誤字数 E が $2E<M$ をみたすなら誤字訂正ができる。

釜賀の用いた暗語得数という用語は暗号製作者らしい命名である。上の定理 1～4 に続いて、釜賀は暗号作成者の立場で半字差、分数字差、といったものを定義している。暗語の集合 C が完全 M 字差とはいわれないが、完全 $M-1$ 字差とは違うものがある。これを半 M 字差暗語集合という。釜賀は単に半字差ということにとどまらず、分数字差というものを定義しようとした。これはやや変わった定義で、十分な定義とは言えなかったようだが、暗号作成に腐心する姿がみえる。筆名加藤正隆の後年の著『基礎暗号学』では分数字差は省かれている。実際的な方法として、暗語集合 C を互いに共通部分のない部分集合の和 $C_1 \cup C_2 \cup C_3 \cup C_4$ に分け、C 全体 としては $M-1$ 字差だが各 Ci は M 字差であるようにし、必要に応ずるように暗語を部分集合 Ci ($i=1,2,3,4$) に配分するという実際的な方法を『基礎暗号学』で説明している。

弥永教授は『字差概論』を見て、このまま博士論文として提出するようすすめたが、戦争が厳しくなり、敗戦後は原中佐、釜賀少佐は軍籍を消して、郷里に逼塞することを命じられ、論文提出は成らなかった。戦時中なら、日本軍部は公開、公刊を許さなかったであろう。本書は日本軍の暗号作成の諸点を記しているのであるから。弥永教授は『字差概論』の表紙を破って保存した。それが講和後釜賀の手に戻され、ただ1部だけが残った。

Shannon の通信理論もない時代に Hamming の符号理論(通信の誤り検出、訂正の理論)に十数年も先んじて、このような理論を作り出したことに驚きを禁じえない。

追加 釜賀は無限乱数主義であった。そのため陸軍の暗号は解読されたことはないと、終生誇りにしていた。彼と一緒に話していた戦時中、彼とは暗号が解けるということとは何かについて話した。無限乱数暗号文にある文をあてはめたとしても、それがもとの暗号文に対する平文であるとは保証されない。つまり無限乱数暗号文が解けるということになると、それは何を意味することになるのか。たとえある暗文に平文が当てはまったと考えたとして、そこからその暗号システムに対する解読の普遍的手続き(アルゴリズム)が得られない。戦時中無限乱数の補給が困難になると、釜賀は特別計算という表を考案した。これはたとえば 1+ 7=5、2+ 4=3、…といった計算表を、暗号組み立て用と翻訳用に作って部隊に配布したのである。

文献中の Booss-Bavnbek&Hoirup 編の本の中では、日本では軍事暗号についての数学者の関与は世界大戦の遅い時期に始まり、しかも、複雑、高級な方法は用いられていなかったと評されているが、当時の日本の数学の状況はドイツの暗号エニグマの解読における A.Turingの貢献と比べることのできるものではなかった。また筆者のルソンにおける米軍暗号の解読業務の体験にてらしてみると、日本軍の上級機関には、いかなる情報を取り、得られた情報をどのように利用するかという情報戦略はなかったと思う。

なお釜賀は戦時中から、陸軍、海軍、外務省の暗号研究、実施などについて、相互に関係を持たず、ばらばらであることについて、憂慮を口にしていた。また現代暗号にも精通し、晩年まで自ら車で外務省に顧問として暗号指導にでかけていた。

釜賀は2003年11月23日、86歳で死去した。

文献

釜賀一夫　字差概論　　(未公刊　1944年頃)

加藤正隆(釜賀一夫)　基礎暗号学　—情報セキュリティのために— Ⅰ　　サイエンス社　1989年

釜賀一夫　大東亜戦争に於ける暗号戦と現代暗号　『昭和軍事秘話』—同台クラブ講演集—
同台経済懇話会　1989年
同台とは参謀本部のあった市ヶ谷台を共にしたという意味だろう。本文では釜賀自身は太平洋戦争といっている。釜賀自身が話をしている点で珍しい記録である。

木村　洋　　戦中の日本暗号解読史における数学者の貢献　第15回　数学史シンポジウム(2004)
津田塾大学　数学・計算機科学研究所　2005年

B. Booss－Bavnbek&　J. Hoyrup　　Mathematics and War　　Birkhäuser　2003
本書に鹿野忠良氏の勧奨と協力によって、「Mathematics and War in Japan」という短文をのせた。

堀　栄三　大本営参謀の情報戦記、—情報なき国家の悲劇—文春文庫
本書はなかなか面白い本である。しかし中央特情部のマニラ派遣や派遣隊長の撤退の日付などに誤りがある。釜賀一夫から直接、堀に訂正を申し入れたが、訂正は行われなかった。

檜山良昭　暗号を盗んだ男　光人社
釜賀一夫からの聞き書きを元に書かれた本だが、当時は学生もうるさいので本名を秘匿することを山本幸一から乞われ、登場者の名をかえたと釜賀が語っていた。そのまま本書から引用しているものもあるので、注意が必要である。

サイモン・シン　暗号解読—ロゼッタストーンから量子暗号まで—　青木薫訳　新潮社　2001年
ストリップやM209はないが、ドイツの暗号機エニグマについてのA. チューリングの仕事をかなり詳しく書いている。著者は『フェルマーの最終定理』という物語本も書いた。

近藤昭氏　暗号戦　(連載)　『偕行』　偕行社　2002年～2005年

有本　卓　　数学は工学の期待に応えうるのか　岩波書店　2004年
Hammingの距離と符号理論に関する簡単な紹介がある。

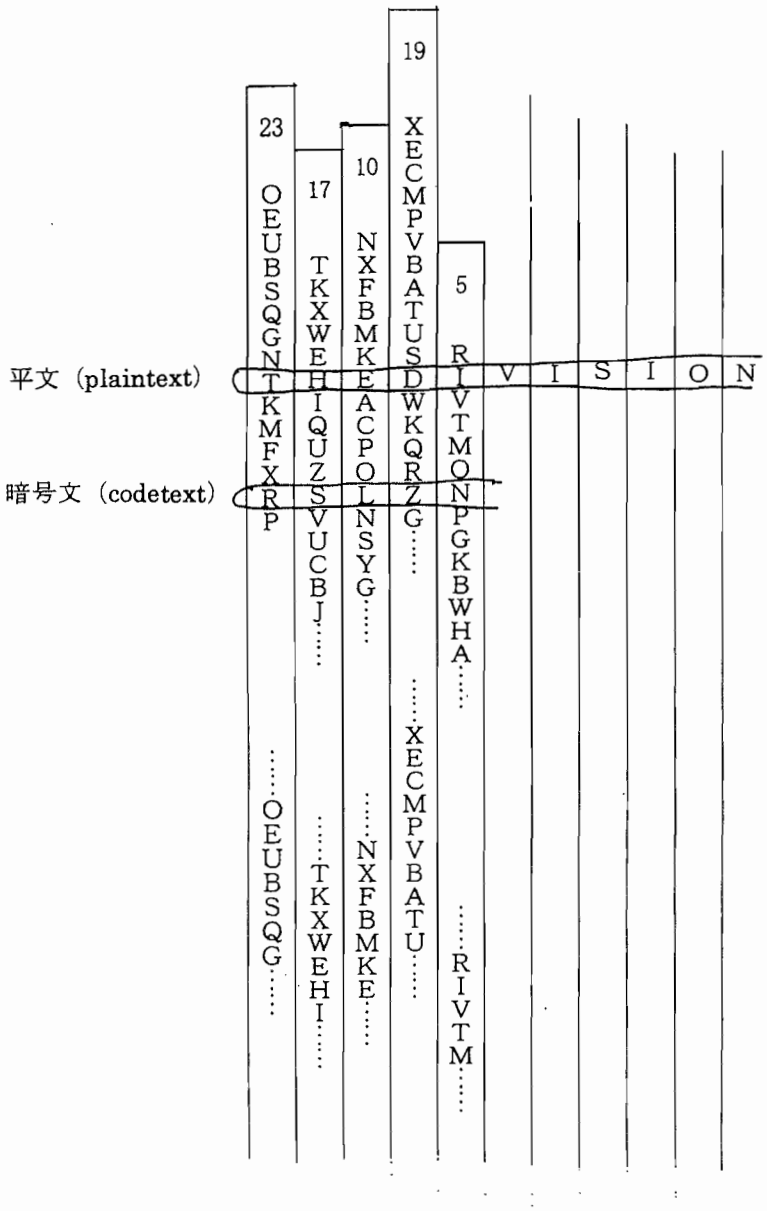
辻井重男　釜賀さんを偲んで　光電技報　第20号　(株)光電製作所　2004年8月

釜賀一夫・辻井重男・佐々木良一・山岸篤弘『釜賀一夫氏の証言』—戦前から現在に至る暗号開発の変遷を語る—　サイファー・セキュリティ・マネージメント　2001年8月号

注　2006年10月14日津田塾大学数学・計算機科学研究所主催の、第17回数学史シンポジウムで表題のような講演をした。その際のレジュメに加筆した。

釜賀一夫氏は生前 レーダー機器・情報通信機器メーカー(株)光電製作所の顧問であった。上記の講演に関し、光電製作所の社員の方々のご協力を頂いた。厚くお礼を申し上げたい。

図1　ストリップ式暗号



（1）Alphabet の permutation を縦に記した棒（strip）を約 100 本 用意し、それに番号を付けておく。

（2）その日ごとに、20～30　本を用意し、どの番号の strip をどういう順に並べて使うかを送信者、受信者の双方が「鍵」として承知している。

（3）図のように各 strip を上、下に移動し平文（plain text）を例えば　ＴＨＥＤ　ＩＶＩＳＩＯＮ……と読めるように並べる。その何段か下（あるいは上）の所を暗号文とする。この図の例では　ＲＳＬＺＮ……。

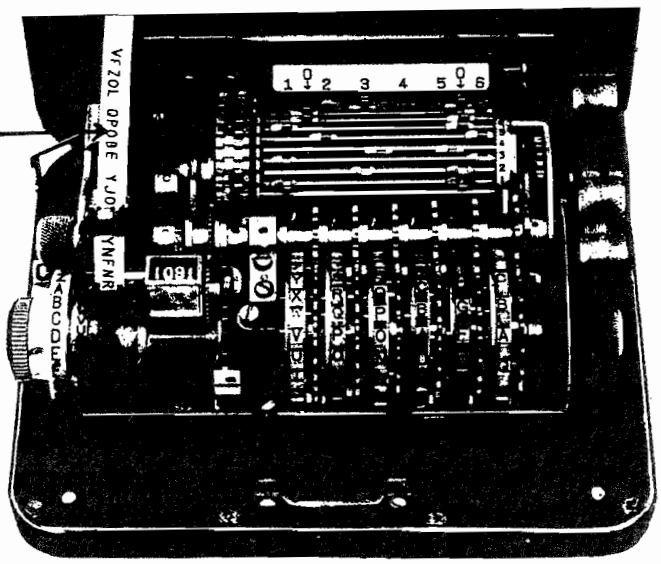
（4）受信者は「鍵」に従って strip を並べ、暗号文が横に並ぶようにすると、その何段か上（あるいは下）に意味のある文が読み取れる。

（5）たとえば図では平文の上３段目には strip 上に文字がない。そのようなことを考慮し、１本の strip には同じ permutation が２本縦に記している。

図2　M２０９暗号機

印字された暗号文のテープ

原文を入力する転輪ノブ



R_i：i 番目の乱字（乱数に相当）　T_i：i 番目の原字（text）
C_i：i 番目の暗字（code）

原文は　語　$T_1T_2T_3\cdots\cdots$　であるとし、暗号文は　語　$C_1C_2C_3\cdots\cdots$になるとしよう。

本機では、以上の文字に対して アルファベットA，B，C，…，Zの順に 数 0，1, 2, …，25 を当てると

$R_i - T_i \equiv C_i \pmod{26}$　という関係の機構になっている。

従って、その機構によって

$R_i - C_i \equiv T_i \pmod{26}$　という関係で原文が得られる。

写真は　加藤正隆著　基礎暗号学 I　サイエンス社　による