MA THEMA TICAL
SCIENCES
September 2000 Number 447

特集／暗号の数理

暗号理論の研究動向

今 井 秀 樹

1. はじめに

暗号は文字の発明とほとんど同時に発明され，今日に至るまで人類の歴史の中で，様々な形で用いられてきた．実用的な暗号は，主として軍事や外交で用いられ，暗号の解読の成否が一国の命運を制したことも少なくない．一方，暗号はクイズや小説などの分野でもしばしば取り上げられてきた．エドガ・アラン・ポーの「黄金虫」は，海賊キッドの宝の隠し場所が示された暗号を解読する過程が面白く書かれている．この暗号は，英文の各文字を図形で置き換えた暗号であった．このような暗号を換字暗号と呼ぶ．もう一つよく知れらている暗号に転置暗号がある．これは，文字の順序を入れ替える暗号で，ことば遊びなどにも用いられるから，読者にも馴染み深いものであろう．この種の暗号とは別に，一見何の変哲もなさそうな普通の文章の中に，秘密の文を埋め込むという暗号も，小説の世界ではよく登場する．例えば，文の各節の頭文字を取ると意味のある語になるといった暗号である．これは秘密が隠されていること自体をわからないようにして，秘密情報を伝達する手法であり，ステガノグラフィーと呼ばれる．著作権保護のための重要な技術として最近注目を集めている電子透かしは，ステガノグラフィーの一種と見ることができる．

近代になって，実用暗号としては，換字と転置を複雑に組み合わせ，それを鍵と呼ばれる記号列によって制御するという方式が主流となり，今日に至っている．このような暗号は最近まで専用の暗号器で処理されることが多かったが，今日ではソフトウェアで処理されることも少なくない．

暗号の構成，解析の理論である暗号学は８世紀頃に，アラビアで始まったとされている．その後，主として欧米で軍事に関わる理論として発展したきたが，1970 年代になって暗号学は全く新たな様相を呈してきた．その契機の一つは，1977 年に米国連邦政府の標準暗号として採用された DES（Data Encryption Standard）であり，もう一つは同じ年に Diffie と Hellman によってその概念が提案された公開鍵暗号である．具体的公開鍵暗号の最初のものは，1978 年に Rivest, Shamir, Adleman により提案され，RSA 暗号と呼ばれた．この時期以降の暗号を現代暗号と呼ぶことがある．

現代暗号誕生の契機となった DES と公開鍵暗号の出現は決して偶然ではない．これらは，1970 年代からの情報通信ネットワークの進展に呼応したものといえる．ネットワークが拡大し，不特定多数のユーザが秘密通信を行うようになれば，誰もが使える標準暗号が必要になってくる．それが DES だったのである．また，大規模なネットワー