

▼多表式暗号

平文	JUL	IUS	CAE	SAR
暗号文	MAQ	LAX	FGJ	VEG
ずらす文字数	365	365	365	365

カエサル暗号を拡張した多表式暗号の例。平文を3文字ずつ区切り、それぞれ3、6、5文字ずつ換字し、これを繰り返す。この区切られる長さ(ブロック)を長くずらす。文字数をランダムにすれば解読はさらに困難になる。

暗号作成時や復号時の変換表による作業を容易にするために、この鍵を自動的に作成する機械が作られるようになり、やがて、タイプ入力するだけで暗号文を出力する装置なども作られるようになった。

これら自動変換をおこなう暗号機械では鍵の長さが長くなり、複数の暗号文を作成してもこの鍵が重複しないように工夫されるようになった。

2-2



物理学者が作った暗号機械

電気抵抗を測る装置、ホイートストン・ブリッジを発明したことで有名な英国の物理学者、ホイートストン(Charles Wheatstone 1802~1875)は磁針電信機や電気時計を考案しているが、彼は円盤式暗号機も考案している。これは大小2枚の円盤を重ね、時計のように取り付けられた長針を大きい円盤(外側)の文字に合わせると、短針が小さな円盤の別の文字を指すといった簡単な構造のものだ。英国がこの暗号機を、英米両軍の前線で使用することを決定したのは1918年の始めであった。そして、このホイートストン暗号機の大小円盤を27と26等分された改良型プレット機が製作され実戦配備された。

このプレット機の唯一の懸念は、この機械がドイツ軍の手に渡った場合のことだけであり、作成された暗号の信頼性は非常に高いものと思われていた。しかし、ワシントンの暗号解読課は最終的な確認のために、リバーバンク研究所の暗号研究チームで安全性のテストをおこなうことを指示した。

暗号研究チームのウィリアム・フリードマン(William Frederick Friedman 1891-