暗号と社会のかかわり史

（株）IT 企画　才所敏明

（１）はじめに

人類の歴史は紛争の歴史ともいえる。暗号は、そのような時代時代の紛争当事者のニーズに応じ、新たな暗号の考案とその解読が繰り返され発展してきた。本稿では、最初の暗号が考案された紀元前 3000 年頃から第二次世界大戦終戦 1945 年頃までの、暗号とその社会とのかかわりの歴史を概観する。

本メモは、暗号・認証技術の研究開発に携わる一員であり戦後世代である筆者が、多くの先人の成果を参考にまとめたものである。人類・社会の歴史の陰に、暗号に関する熾烈な戦いが存在し、その勝敗が人類・社会の歴史を形作ってきたことをご理解いただければ幸いである。

（２）古代暗号

①ヒエログリフ

現存する最古の暗号は紀元前３０００年頃のヒエログリフといわれている。ヒエログリフは、ヒエラティック、デモティックと並ぶエジプト語の表記体系の一つで、象形文字の一種。ヒエラティックはヒエログリフの崩し字体で、主に行政文書、法的文書、学術的文書に、デモティックはヒエラティックがさらに簡略化された字体で、主に世俗的な書き物に使われた。それに対しヒエログリフは、石碑や神殿、墓などに文字を刻むときに使用される神聖な文字であった。長年ヒエログリフの解読ができなかったが、19 世紀にロゼッタ・ストーンの研究が進展し、それが突破口となり解読された。

ヒエログリフは刻んだ文字や内容の秘匿を目的としたものでは無く、ヒエログリフで刻まれた内容が長年解読できなかったため「暗号」として扱われることもあるが、機密情報の秘匿を目的としたいわゆる「暗号」とは異なる。

図１．古代エジプトの墓碑に刻まれたヒエログリフ

https://commons.wikimedia.org/wiki/File:Egypt_Hieroglyphe2.jpg

②スキュタレー暗号

紀元前 600 年頃、古代ギリシャの都市国家・スパルタでは「スキュタレー暗号」が用いられていた。スキュタレー暗号は、ある太さの棒（スキュタレー）に革紐を巻きつけて棒に沿って革紐に文字列（平文）を書くことにより革紐上に暗号文が作成（暗号化）され、同じ太さの棒にその革紐を巻きつけることにより送り手が書いた文字列が棒に沿って現れる（復号できる）という仕組みである。棒の太さが異なれば文字列の順序が変わり正しい文字列が現れず、使用する棒の太さをあらかじめ送り手と受け手の間で取り決めておくことにより、その棒の太さを知っている受け手のみが送り手が書いた文字列（平文）を正しく読める、という暗号方式である。

このように、文字を読む順番を並べ替えることによって暗号化する方式を「転置式暗号方式」という。

図２．スキュタレー

https://commons.wikimedia.org/wiki/File:Skytale.png

③シーザー暗号

紀元前 100 年頃に登場したシーザー暗号は、古代ローマの軍事的指導者ユリウス・カエサル（ジュリウス・シーザー）が頻繁に利用したことから名づけられた暗号方式である。シーザー暗号は、元の文章（平文）のアルファベットをある数だけずらして暗号化するもので、同じ数だけアルファベットを逆側にずらすことにより元の文章を復元（復号）できる。アルファベットをずらす文字数をあらかじめ送り手と受け手の間で決めておくことにより、そのずらす文字数を知っている受け手のみが、送り手が書いた元の文章（平文）を読める、という暗号方式である。

このように、一定のルールで文字を入れ替えて暗号化する方式を「換字式（かえじしき）暗号方式」という。

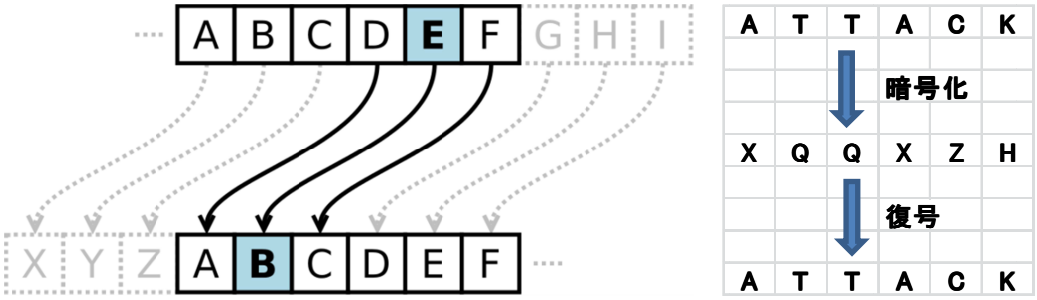

図３．シーザー暗号（3 文字左へシフト）による暗号化/復号の例

https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg

（３）古典暗号（外交活動の活発化による暗号の普及期へ）

①ノーメンクラタ暗号（女王メアリ暗号）

シーザー暗号に代表される「単一換字式暗号」は、アルファベット１ 文字につき別の１ 文字しか割り当てられず、文字の出現頻度分析等により簡単に解読される宿命にあった。ノーメンクラタ暗号は、アルファベットを置き換える他に、フレーズを記号などに置き換える操作を加え、あらかじめ送り手と受け手でフレーズと記号の置き換えのルールをまとめた「コードブック」を共有することにより、その「コードブック」を持っている受け手のみが元の文章（平文）を読める、という暗号方式である。

このノーメンクラタ暗号は、16 世紀、スコットランド女王メアリ・スチュアートがイングランドのエリザベス女王暗殺を企て、その共謀者とのやり取りに利用した暗号として有名であり、エリザベス女王の側近のウォルシンガム配下のスパイ組織網により暗号文が入手され暗号解読の名人に解読され、女王メアリは処刑された。ノーメンクラタ暗号が女王メアリ暗号と呼ばれる所以はここにある。

なお、ウォルシンガムは解読の事実を伏せ、メアリにはしばらく手紙のやり取りを行わせ、メアリがエリザベスの暗殺を手紙に記したのを見計らって（確実な証拠を確保の上）メアリと共謀者を一網打尽にし、全員を処刑した。敵対勢力の暗号化された通信から情報を継続入手するため暗号解読の事実を伏せることは、以降の歴史でも良く採られた方法である。

②ヴィジュネル暗号

ノーメンクラタ暗号は、膨大な「コードブック」の準備と送り手と受け手による「コードブック」の共有が課題であった。15 世紀頃から、二つ以上の暗号アルファベットを使う「多表式」の換字式暗号の研究がはじまり、16 世紀になって強力なヴィジュネル暗号がフランスの外交官ブレーズ・ド・ヴィジュネルにより考案された。

ヴィジュネル暗号は、ヴィジュネル方陣と呼ばれる文字を要素とする 2 次元の換字表（ピンク部分）を用いる方式である。暗号化すべき平文内の文字 1 文字ごとに、ブルー欄内のその文字が示す行と、暗号化すべきその文字の位置にある鍵文字列内の文字 1 文

字がグリーン欄内のその文字が示す列が交差する、2 次元換字表の位置にある文字（ピンク部分の文字）に置き換える、という暗号方式である。なお、鍵文字列が平文の文字列より短い場合は、同じ鍵文字列が繰り返し使用される。

平文文字＼鍵文字	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

図４．ヴィジュネル方陣の例

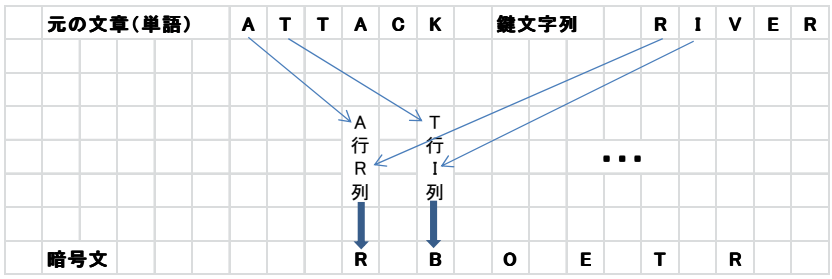

図５．図４のヴィジュネル方陣を利用した暗号化プロセス

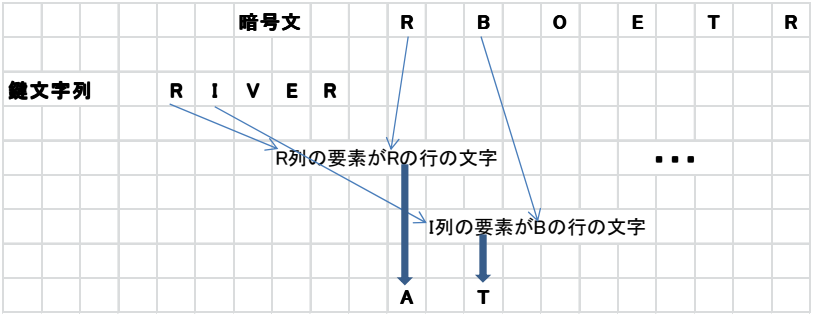

図６．図４のヴィジュネル方陣を利用した復号プロセス

このヴィジュネル暗号は、万一、換字表が第三者に渡っても、鍵が異なれば全く別の暗号文に変換されるので、鍵が分からなければ解読は難しい。

ヴィジュネル暗号は、19 世紀のアメリカ南北戦争において、合衆国を脱退した南部 11 州で結成した連合国軍側の標準暗号として使用された。

③上杉暗号

16 世紀には、日本でも方陣を用いた暗号が編み出されている。上杉暗号は、戦国時代の武将、上杉謙信の軍師だった宇佐美定行が著した兵法書に暗号の作り方が記されている。いろは 48 文字を 7×7 のマス目（ブルー部分）に書き、1 文字を行（イエロー欄）と列（グリーン欄）に割り当てられた数字で表す暗号方式で、換字式暗号の一種である。

七	六	五	四	三	二	一	
ゑ	あ	や	ら	よ	ち	い	一
ひ	さ	ま	む	た	り	ろ	二
も	き	け	う	れ	ぬ	は	三
せ	ゆ	ふ	ゐ	そ	る	に	四
す	め	こ	の	つ	を	ほ	五
ん	み	え	お	ね	わ	へ	六
	し	て	く	な	か	と	七

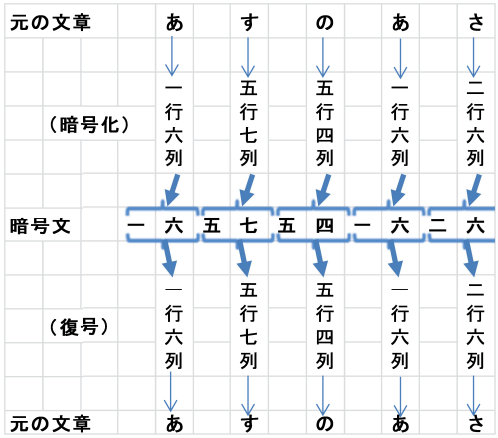

図 7．上杉暗号の方陣例と暗号化・復号プロセス

（4）近代暗号（暗号の作成・解読は、手作業から機械へ）

①ツインマーマン暗号

第一次世界大戦（1914 年～1918 年）開戦当時、ドイツの外務大臣ツインマーマンは、各国のドイツ大使に指令を出していた。イギリスがドイツへ宣戦布告をすると同時にドイツの海外用海底通信ケーブルを切断したため、ドイツ軍は傍受されるリスクが高いイギリス経由の国際ケーブルか無線を使うしかなくなり、通信内容を暗号化し敵国への情報漏洩の防止を図った。しかし、通信は傍受され、イギリスの暗号解読の専用機関（通称、「40 号室」）にて解読された。

開戦当時、ドイツにとってアメリカのヨーロッパ戦線参戦は戦争の行方を左右しかねず、ツィンマーマンはアメリカの参戦意欲を削ぐためにメキシコと日本にアメリカを攻撃させるという構想を立て、ワシントン駐在のドイツ大使に工作指示を出した。しかし、それもイギリスに傍受され「40 号室」によって暗号は解読された。

解読に成功したイギリスは解読結果の公表を避けた。その理由は、イギリスがアメリカの通信を傍受・解析していることは知られたくない、ドイツがより強力な暗号開発に取り組みことを避けたい、成功した解読手法により傍受を継続したい、ためである。結局、イギリスはメキシコ電信局に忍び込んだスパイによってドイツ大使館からメキシコ

に送られた平文の電報を入手しアメリカへ提供、アメリカはドイツに宣戦布告し、ヨーロッパ戦線に参戦した。

②ADFGX 暗号

1918 年、第一次大戦の終盤に、ドイツ軍のフリッツ・ナベル大佐が考案した ADFGX 暗号が使われた。ADFGX 暗号は、行と列には ADFGX の 5 つの文字を割り当て、行列内の要素として定義された 1 つの文字を、行と列に割り当てられた 2 つの文字に置き換え（上杉暗号と同じ仕組み）で、その上で得られた文字列に対して、さらに転置式暗号方式を用いて暗号化する。ADFGX 暗号で 5 つの文字が使われた理由は、モールス信号での送信の際にいちばん識別しやすいため、といわれている。

この ADFGX 暗号を解読したのが、フランス暗号局のジョルジュ・ペーバン大尉である。5 つの文字しか使われていないことから、マス目の暗号であると推定し、そして位置の入れ替えも行われている事を見破り、3 週間の不眠不休の努力によって、これを解読した。この暗号の解読がドイツの敗北の遠因であったとも言われている。

	a	d	f	g	x
a	D	I/J	N	F	S
d	H	A	O	G	E
f	R	Q	B	W	L
g	C	Y	M	U	V
x	Z	P	X	T	K

図 8．ADFGX の行列例

③エニグマ暗号

暗号は19 世紀まで手作業で作成されていたが、20 世紀に入ると機械式暗号機の登場し、暗号解読の難易度が飛躍的に増すことになった。その中でも傑作と言われたエニグマは、1918 年にドイツの発明家アルトゥール・シェルビウスによって発明された機械式暗号機で、携行性と機密性を売りにして販売されたが、当初、ドイツ軍は第一次世界大戦で使用していた暗号が解読されていた事実を知らず、より強力な暗号が必要という意識は低く、また高価であったこともあり、ドイツ軍は採用しなかった。しかしその後、イギリスによって暗号が解読されていたことで第一次世界大戦に敗れたと知ったドイツは、暗号が国家の存亡を左右するという危機感から、エニグマ採用を決定した。

エニグマの暗号方式は多表式換字式暗号で、「スクランブラー」と呼ばれるアルファベット 26 文字が刻まれた数枚の歯車（ローター）と、プラグボードと呼ばれる単文字変換を行う仕組みの組み合わせが「鍵」となる。スクランブラーをセット後、平文をキーボードで打つと、スクランブラーを通じて暗号化された文字がランプボードに表示さ

れる。スクランブラーは1文字打つごとに1目盛り回転することによって、1文字ごとに異なる鍵を使って暗号化することになる。

ヒトラーが政権を握った後、ドイツは5個あるスクランブラーの中から3個を選んで組み合わせたり、3個しか設置できなかったスクランブラーを最大5個まで設置可能にしたりなど、エニグマの改良を施し使用していた。

ドイツが信頼していたエニグマであったが、当時ドイツから侵略の脅威にさらされていたポーランドは、その解読方式を見出し「ボンブ」という解読機を発明していた。ポーランドの暗号局「ビュロ・シフルフ」に所属していた数学者マリヤン・レイェフスキは、同じ日に出された複数の暗号文を比較して、暗号文の冒頭に出てくる6文字が「メッセージ鍵を送るためで、3文字が2回繰り返されている」ことを発見する。これを突破口にして、スクランブラーの初期設定と文字の出現パターンの対応表を作成し、解読に成功した。しかし、ドイツがエニグマを改良することによって増大する暗号パターンにポーランドが対応できず、資金的にも人材的にも充実しているイギリスにその研究情報を渡し解読を託した。その2 週間後に、ドイツはポーランドへ侵攻、第二次世界大戦（1939年～1945年）が始まることになった。

エニグマ暗号の解読作業が難航していた英国だったが、ポーランドの「遺産」を引き継ぎ、MI6（英国情報局秘密情報部）の拠点であるブレッチレーパークでエニグマ解読に当たった。ブレッチレーパークに集められた精鋭の中でも、ひときわ才能を発揮したのが数学者のアラン・チューリングだ。1940年には改良したボンブを使用してエニグマの暗号解読に成功している。イギリスがエニグマ暗号を解読して得たドイツに関する情報は「ウルトラ」と呼ばれ、終戦まで連合国にとって貴重な情報源となったが、エニグマ暗号解読の事実は極秘事項として扱われ、ドイツは終戦までエニグマを信頼して使用し続けていた。エニグマ暗号が解読されていたという事実が公表されたのは、解読から20 年以上も経過した1974 年のことであった。

なお、大戦中、ヒトラーと将官たちの通信は、エニグマよりもさらに強力なローレンツSZ40暗号機によって暗号化されていたが、アラン・チューリングはローレンツ暗号を解読するための技法Turingeryを1942年に考案、電子工学の研究者トミー・フラワーズがコロッサスと呼ばれる暗号解読用のコンピュータを完成させ、ローレンツ暗号の解読に使用された。戦後、イギリスは戦時中の秘密を守るためにコロッサスの設計図を焼却し、関係者は固く口止めされ、近年までコロッサスの存在はほとんど知られていなかった。そのため、世界初のコンピュータは一般にはENIAC（1946年）とされているが、暗号解読用とはいえ、コロッサスは1943年には稼働していた。

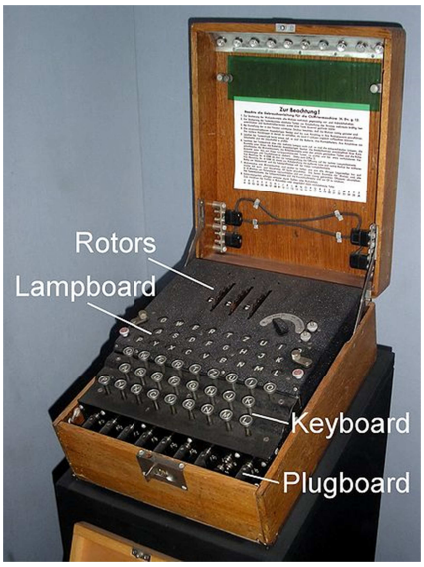

図９．エニグマ暗号機

https://commons.wikimedia.org/wiki/File:EnigmaMachineLabeled.jpg

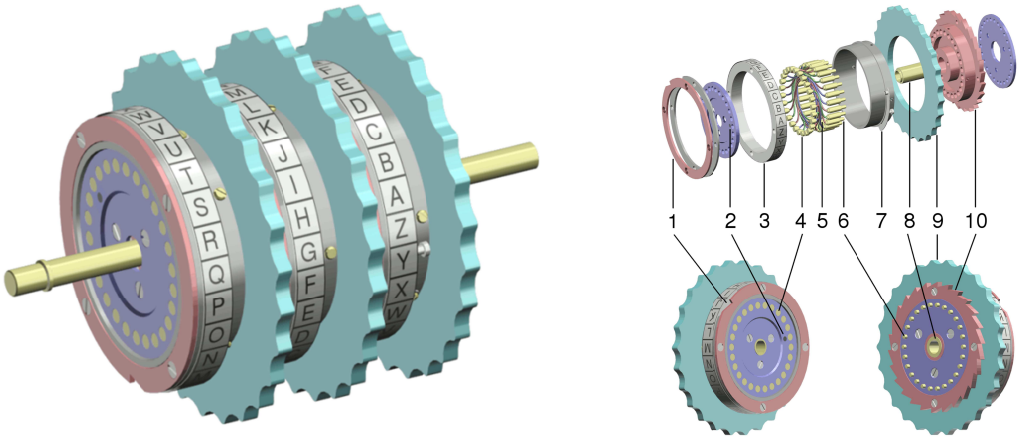

図１０．エニグマの内部のローター

https://commons.wikimedia.org/wiki/File:Enigma_rotor_set.png

④パープル暗号（九七式暗号）

太平洋戦争中（1941 年～1945 年）、日本の外務省は海外公館との連絡に使用していた暗号方式である。パープル暗号（日本では「九七式暗号」）は海軍技術研究所が開発したもので、暗号機はプラグボード、切り替えスイッチ、タイプライターの 3 つのパートで構成され、日本版エニグマとでも言うべき精巧な暗号機であった。しかし、アメリカのフリードマンの指揮する解読班によって 1940 年にはその原理が見破られ、コードブックも日本総領事館から盗撮され、日本の暗号はアメリカ側に筒抜けになっていた。

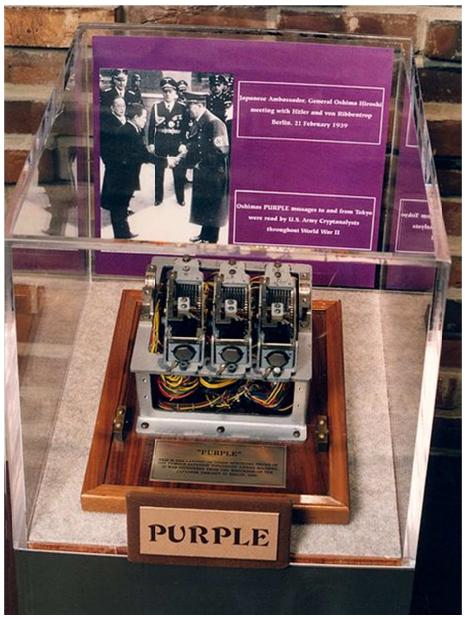

図１１．米国立暗号博物館に展示されている捕獲部品

https://commons.wikimedia.org/wiki/File:PURPLE.jpg

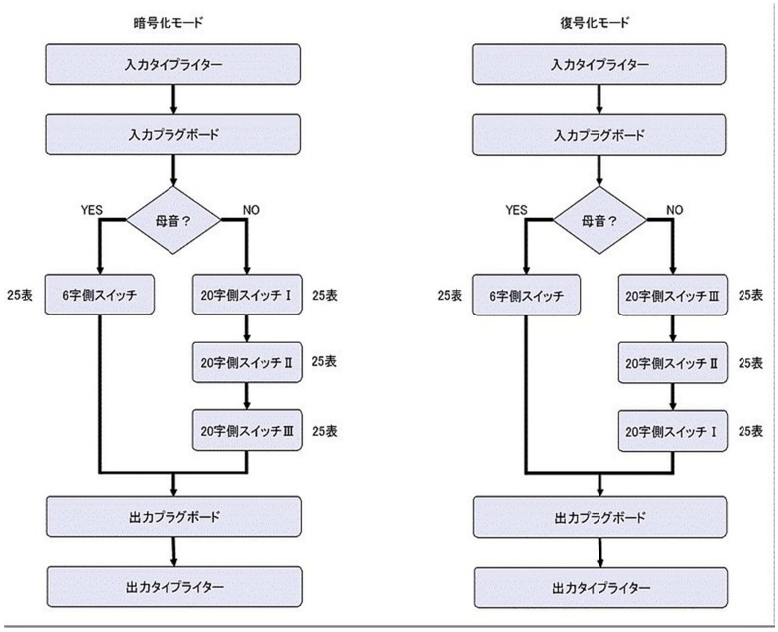

図１１．パープル暗号機の模式図

https://ja.wikipedia.org/wiki/%E3%83%95%E3%82%A1%E3%82%A4%E3%83%AB:Purple_diagram.jpg

⑤ミッドウェー暗号（海軍 D 暗号）

太平洋戦争のターニング・ポイントとなった、ミッドウェー海戦。それまで、勇戦を続けてきた帝国海軍は、機動部隊の主力をこの作戦に投入した。しかし奇襲作戦は失敗し、逆に奇襲攻撃を受け、虎の子の空母 4 隻を失う結果になった。このとき帝国海軍が使用していた「海軍暗号書 D（海軍 D 暗号）」は大変複雑な暗号であったが、アメリカ軍はすでに

日本の通信暗号を数多く集めており、乱数表も撃沈された潜水艦などから入手していたので、暗号解読によって帝国海軍の手の内すべてを察知しており、満を持してミッドウェー島北方洋上で待ち構えて奇襲攻撃をかけたのであった。

（５）おわりに

転置式暗号、単一換字式暗号、コードブック式暗号、多表式暗号、鍵付き多表式暗号、およびその組み合わせなど、暗号が次々と考案されまた次々と解読され、それぞれの時点の紛争・戦争の勝敗を大きく左右し、人類の歴史を築いてきた。

第二次世界大戦終戦とともに、暗号とその利用も大きく変わることになる。しかし、それまでの暗号を構成する要素技術（仕組み）は、現代の共通鍵暗号技術に脈々と引き継がれているのである。

以上

参考資料

①簡単にわかる暗号の歴史　Symantec Corporation

https://www.jp.websecurity.symantec.com/welcome/pdf/wp_encryption_history.pdf

②暗号の歴史　三菱電機（株）

http://www.mitsubishielectric.co.jp/security/learn/info/misty/

③日米暗号戦争の総括（元日本軍将校　寺井義守著）

http://ktymtskz.my.coocan.jp/E/EU4/code18.htm

④ツインマーマン電報事件　海洋戦略研究

http://blogs.yahoo.co.jp/hiromichit1013/28319467.html

⑤エニグマ（暗号機）　ウィキペディア

https://ja.wikipedia.org/wiki/%E3%82%A8%E3%83%8B%E3%82%B0%E3%83%9E_(%E6%9A%97%E5%8F%B7%E6%A9%9F)

⑥パープル暗号　ウィキペディア

https://ja.wikipedia.org/wiki/%E3%83%91%E3%83%BC%E3%83%97%E3%83%AB%E6%9A%97%E5%8F%B7