＜冬休み前 レクリエーション(シーザー暗号)＞

考えてみよう！①

クリスマスの夜、サンタクロースは子供たちにプレゼントを配っていました。プレゼントを配るために、花子さんの寝室にサンタが侵入したところ、枕もとの欲しい物メモには、以下のようなメッセージが書かれており、何の動物のぬいぐるみが欲しいか暗号化されています。サンタはメモから、欲しいぬいぐるみの動物を 3 つまで絞れたようです。花子さんが欲しいプレゼントを考えてみましょう。

サンタさんへ

欲しいものは、
DBU のぬいぐるみ
です。

ヒント：DBU は動物です。

花子

① DOG(犬)
② CAT(猫)
③ FOX(狐)
のどれかじゃろうな…
早く見つけないと次の家
に進めないんじゃ～！

※ イラストは Gemini 3 Pro を使用。

花子さんが欲しい物：（　　）

○ シーザー暗号

先ほどの花子さんの暗号のように、決まった文字数分のアルファベットをシフトさせて、行う暗号を、**シーザー暗号**とよぶ。

シーザー暗号は、古代ローマの軍人・政治家であった、ガイウス・ユリウス・カエサルが使用したことから、この名前になった。カエサル(Caesar)の英語読みがシーザーだからである。ちなみに、カエサルは「賽は投げられた」や「ブルータス、お前もか」など、色々な名言を残していることでも有名である。

やってみよう！ ①

アルファベットの表を埋めながら、以下の問題に答えよう。

(1) 「HAL」をいくつ分右にずらすと、「IBM」になるか。

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

答え：（　　）

(2) 「CHEER(応援する)」を７文字右にずらすとどのような単語になるか。

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

答え：（　　）

○ シーザー暗号と数学

シーザー暗号は、最もシンプルで広く知られた暗号である。暗号は、数学の一分野として考えることができる。ここからは、シーザー暗号を式として表してみよう。

考えてみよう！②

以下のように、アルファベットを数字に変換します。暗号化する文字の数字をx、暗号化された文字の数字をyとしたとき、9文字右にずらすシーザー暗号は、どのような式で表せるのでしょうか？

ヒント：「sleep(眠る)」と「bunny(ウサギ)」を例として、変換を考えてみよう。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

※ 0からスタートしていることに注意!

（答え、工夫点、上手くいかない理由など）

シーザー暗号の式を単なる足し算で表現すると、番号が 25 を超えてしまい、上手く変換できない。

実は、シーザー暗号は割り算のあまりの考え方を使うと、数式として表現できる。

割り算のあまりを求める計算として、mod がある。mod の計算では、整数mを自然数nで割ったあまりをrとしたときに、$\boldsymbol{m \bmod n = r}$ となる。

例）5 mod 10 = 5、12 mod 10 = 2 とか。（$m < n$のとき、$m = r$）

※ mod は一応、数学 A で扱う。しかし、必須ではなくなったので、ここで説明

この考え方を使うと、9 文字右にずらすシーザー暗号は、以下のようになる。

（　　）

やってみよう！②

mod の式で変換の式を表現し、以下の表を利用して暗号を解読してみよう。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

(1) 「TERRA(地球)」を 13 文字右にずらすとどのような単語になるか。

答え：（　　）

(2) 「COLD(寒い)」を 3 文字右にずらすとどのような単語になるか。

答え：（　　）

○ 複雑なシーザー暗号

シーザー暗号では、暗号を解く際に、何文字ずらすかという数字が重要になる。暗号ではこのような数字を**鍵**という。また、この鍵がばれてしまうと、だれでも暗号を解けるようになってしまう。暗号は解くべき人以外には解かれたくないので、鍵がばれるのは非常に困る。

シーザー暗号は、暗号化する鍵と、暗号を解く鍵が一緒であるため、**共通鍵暗号方式**とよばれる。

シーザー暗号の鍵は、0～25 の 26 通りであるため簡単に解かれてしまう。そのため、キーワードを使って、アルファベットの表の並び方を変える方法も存在する。

例えば、「JUNSHIN」をキーワードとする。次に複数現れる n を削除して、「JUNSHI」とする。この文字列を表の最初に置き、それ以降は残りのアルファベットを順に表に追加する。

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

そして、この表を使って暗号化と暗号を解く。この表を使って、「CAT」を一文字右にずらすと、「NJR」に変換できる。

この場合、鍵は I と「JUNSHIN」であり、普通のシーザー暗号よりは鍵を知らない人に解かれづらくなる。

やってみよう！ ③

好きな言葉と好きな数字をキーワードにして、暗号を作ってみよう。また、近くの人と暗号を交換し、解いてもらおう。

キーワード：（　　）　右にずらす単語数：（　　）

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

暗号：（　　）

答え：（　　）

○ 暗号とこれから

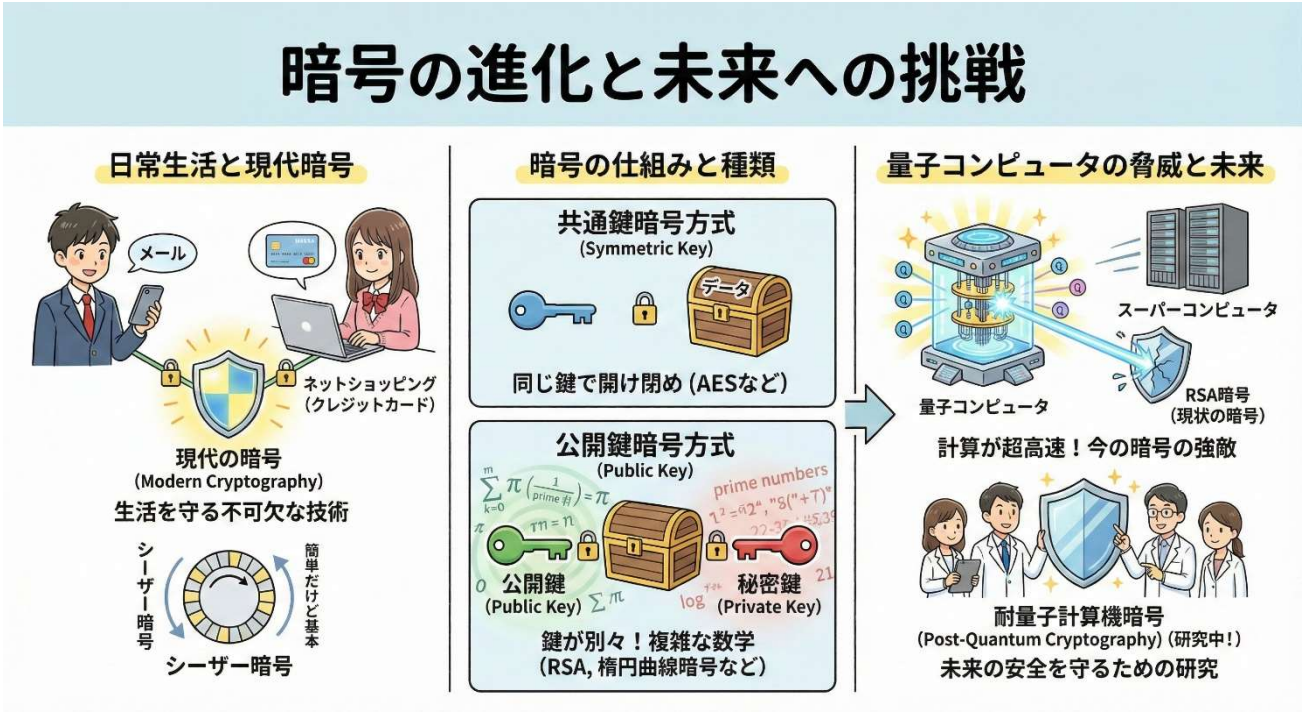
暗号は、メールでの情報交換、クレジットカードでの買い物など日常生活を安全に送るために必要不可欠な技術である。

今回紹介した、シーザー暗号はとても簡単だったが、今の社会で使われている暗号はもっと複雑で、難しい数学の考え方がたくさん使われている。公開鍵暗号方式(暗号化する鍵と暗号を解く鍵が一緒)では、**RSA 暗号**や、**楕円曲線暗号**が有名である。共通鍵暗号方式では、**AES** が最もよく使われている。

暗号は、コンピュータの性能との勝負である。今ある暗号も、計算がとても速いコンピュータができれば、解かれてしまう。実際に、RSA 暗号は現状のコンピュータでも解かれてしまう可能性があり、徐々に使われなくなっている。

今のコンピュータよりも、計算がとても速くできるコンピュータとして、**量子コンピュータ**がある。量子コンピュータはまだ研究段階であり、完成していない。

量子コンピュータは計算が速いため、色々な分野での活躍が期待されるが、暗号にとっては恐ろしい敵である。そのため、今は量子コンピュータが実用化されても、解かれない暗号が研究されていたりする。



※ イラストは Gemini 3 Pro を使用。