小学生のためのRSA暗号入門教室

※RSAは開発したMIT(マサチューセッツ工科大)の３名の研究者の頭(かしら)文字です。
リベスト，シャミア，アドルマン

＜ねらい＞
暗号には，算数(数学)が利用されていることやその仕組(がいよう)を理解しよう。

令和３年２月５日
亘理町立高屋小学校

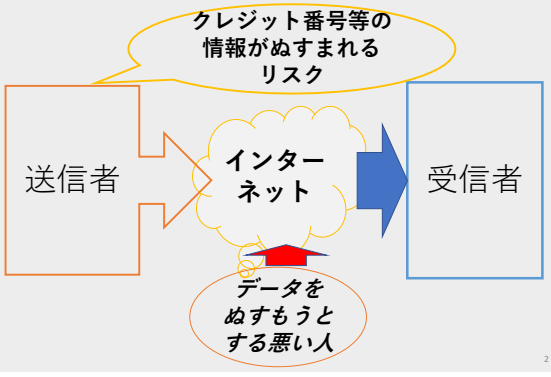
1

どうしてあまりの数字からもとの数字がわかるのかな?

「デジタル化」社会はブラックボックスが多くないですか?

4

データ暗号はどうして必要なの?



2

数字当てゲームについて

ある数をAとすると，
3回かけるから ⇒ A×A×A
これを33でわるから ⇒ A×A×A÷33 だね。
あまりが〇〇。でも，商がわからないよ。

あまりを1で考えようか。商をB とすると，
A×A×A÷33＝B あまり1
ということは，
A×A×A＝B×33＋1

Aをみつけることはむずかしいね。

だから，ぬすむのがむずかしい暗号なのかなぁ?
でも何か種(たね)があるんだよ!?。

5

１～３２までの数字の中から好きな数字をえらんでみよう。

あなたのえらんだ数字 ○

その数字を３回かけてください。
○×○×○＝□
その後，３３でわってください。
□÷33＝□
あまりの数字のみを教えてください。

3

むかしの暗号

例:シーザー暗号など

古代ローマの将軍カエサルのことだね。紀元前1世紀ころの人だよ。

シーザーは３文字ずらしたようだけど，
１文字ずらしの例を見てみよう!

もとの文	I	?	A	M	?	B	A	C	K
暗号文	J	?	B	N	?	C	B	D	L

暗号を見破るのはかんたんかもしれないね。

6

かんたんな暗号の練習

『問題①』
「ＫＯＹＡ」を3文字ずらして，暗号化してみよう。

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
3文字ずらすと																									

もとの文: ＫＯＹＡ

暗 号 文:

7

問題② 暗号文をどのように指示すれば もとの文にもどせるかな?

あなたが伝えたい内容	H	E	L	L	O
	T	O	K	Y	O
	?	?	?	?	?

あなたが送った暗号 HT?EO?LK?LY?OO?

8

現在使われている暗号化のしくみ ＝ＲＳＡ

データを送信するＡさんは鍵(かぎ)を使って暗号化してから送ります。

データを受信したＢさんは秘密の鍵(かぎ)を使って，元のデータに戻します。

9

RSA暗号の練習①

２つの素数p=「３」とq=「１１」を使ってＲＳＡ暗号の「公開鍵」と「秘密鍵」を作ってみましょう。

手順(アルゴリズム)・・・*数学者が考えたんだね。すごいね!*

① ｎ＝ｐ×ｑ を求めましょう。

② ｐ－１とｑ－１を求めましょう。
ｐ－１＝ ｑ－１＝

③ ②で得た「ｐ－１」と「ｑ－１」の最小公倍数Ｌを求めましょう。

10

④ ③で求めた最小公倍数Ｌとの最大公約数が１になる(互いに素といいます。)数字ｒを求めましょう。
最大公約数が１ということは１以外に公約数がないんだね。

公開鍵ができましたよ。公開鍵は(ｎ，ｒ)です。

⑤ ④で求めたｒとかけ算した積を③で求めたＬでわったときのあまりが「1」となる整数ｓを求めます。
つまり，ｒ×Ｓ÷Ｌのあまりが「1」となるｓです。

秘密鍵ができましたよ。秘密鍵は(ｎ，ｓ)です。

11

RSA暗号の練習②

実際に計算してみましょう。
あなたの誕生日の月を相手に送るために，公開鍵を使って暗号をつくります。
① あなたの誕生月の数字を３回かけて，それを３３でわったあまりを計算してください。

② 送信されてきた暗号の数字から，秘密鍵を使ってもとにもどしてみてください。(秘密鍵は７回かけて３３でわる。)

12

実際の鍵(かぎ)は・・・
たとえば,

	×回数	わる数
公開鍵 （送る側）	４８６１１	１８５１７９
秘密鍵 （受け取る側）	１１９６９１	１８５１７９

13

９と２は「7」をわる数（法）として
同じなかまの数といえます。

９を何十回かけるよりも，
２を同じ回数だけかけた方が
計算は楽だよね。

コンピュータも同じなんだよ。

16

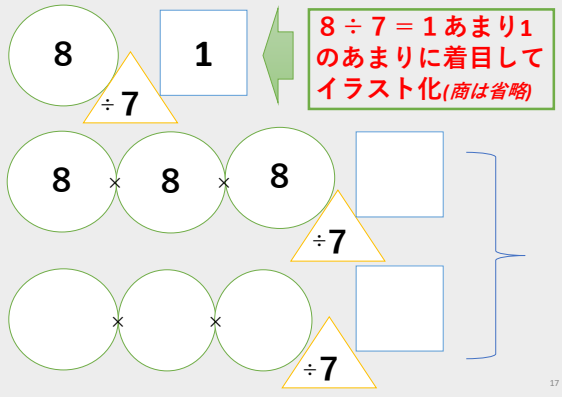
たくさんかけるときどうすればいいの？

下の表を見て気づいたことを話し合おう。

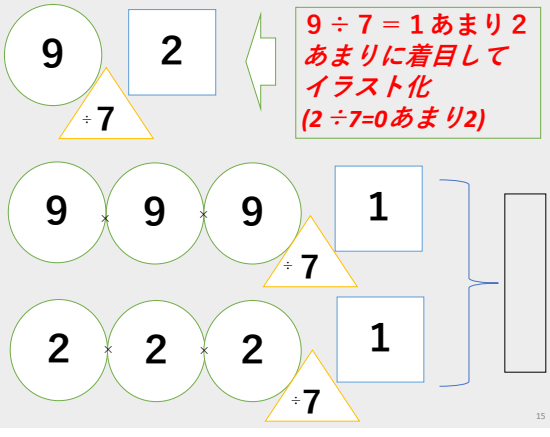
かける回数		「7」あまりで割った	あまりだけを同じ回数だけかけて，「7」でわったあまり
1	9	2	2÷7のあまりは「2」
2	9×9	4	2×2÷7のあまりは，「4」
3	9×9×9	1	2×2×2÷7のあまりは「1」
4	9×9×9×9	2	2×2×2×2÷7のあまりは「2」
5	9×9×9×9×9	4	2×2×2×2×2÷7のあまりは
6	9×9×9×9×9×9	1	2×2×2×2×2×2÷7のあまりは
7	9×9×9×9×9×9×9	?	2×2×2×2×2×2×2÷7のあまりは

14

練習③してみよう！



17



15

今日の授業のまとめ

現代の暗号のしくみには，算数・数学がフルに活用されています。

ＲＳＡ暗号のしくみでは，たとえば，

① 素数(そすう)
② わり算のあまり
③ 最小公倍数
④ 最大公約数など

です。

数学は何の役に立つのかな?

現代人は数学ぬきでは暮らしていけないほどです。

18