これは楽しい数学マジック！

―第3回―

数学で実現　～テレパシーから手品まで、超速算術も～

森井昌克

morii@eedept.kobe-u.ac.jp

（**神戸大学大学院　工学研究科**）

これは楽しい数学マジック！

数学で実現　～テレパシーから手品まで、超速算術も～

- 本日の主題
  - 速算術
    - 文字通り、早く簡単に計算する方法
    - 複利計算：　72の法則
    - おつりを簡単に求める？
  - 手品
    - トランプ手品
  - テレパシーと暗号？
    - 以外と身の回りにある暗号

テレパシーと暗号は時間がかかりそうなので？

専門は暗号なんです！？

暗号は数学の応用！

速算術

複利計算

- １００万円を１％で１０００年預ければ、いくらになる？

$$100万円 \times (1.01)^{1000} = 2億円$$

複利計算

- 低金利時代ですが、バブルの時は年利５％という定期もありました。
- 金利が年５％とは、１万円を預ければ１年後に１万５百円になります。
- ２年後には１万１千円ではなく、この１万５百円に利子５％がつく事にまります。これを複利といいます。
- 年利５％で１万円を預けた場合、倍の２万円になるには何年かかるでしょうか。

複利計算

預入額をz円、年利をr%とするとn年後の金額yは

$$y=z\left(1+\frac{r}{100}\right)^n$$

となります。したがって、

$$2=1\bullet\left(1+\frac{5}{100}\right)^n$$

これを解くと**14.2**となって約１４年かかることがわかります。

複利計算

逆に１０年で２倍になるには年利何%にすれば良いのでしょうか。

$$2=1\bullet(1+\frac{r}{100})^{10}$$

となり、これを解くと**7.15**%と簡単に求められます。

72の法則

- 72の法則とは、元本を2倍にする際の年数と金利を求める方法です。正確ではありませんが、簡単におおよその値をもとめることができます。それは　（金利）[%]×（年数）[年]＝72

金利[%]	69の法則[年]	72の法則[年]	計算値[年]
10	7	7	7
5	14	14	14
2	35	36	35
0.5	138	144	139
0.1	690	720	693

複利計算の雑学？

- 少しの努力でもそれを続ければ大成し、少しでも気を抜き続ければ皆無となる！
  - それを数学的に証明すると？

複利計算の雑学？

- 少しの努力(1.01)を2回続けても

$$1.01 \times 1.01 = 1.020$$

- でもそれを100回続けると

$$1.01^{100} = 2.705$$

- 少し手を抜く(0.99)ことを2回続けても

$$0.99 \times 0.99 = 0.980$$

- でもそれを100回続けると

$$0.99^{100} = 0.366$$

おつりの速算術

- 768円の買い物で1,000円でのおつりは？
  - 1000-768=232
  - 999から引いて、1を加える
    - 999−768+1=232
- 足し算を引き算に？
  - 37＋88＝125
  - 37＋(100−12)＝37−12＋100＝125

カードマジック

トランプマジック

- トランプを使って、カード当てゲームを行う。
  - トリックのタネは数学

テレパシーと暗号

知られていない暗号の世界

ー実は身近に溢れている暗号とその仕組みー

千里ライフサイエンスフォーラム

2012年12月20日

森井昌克

morii@ieee.org

（神戸大学大学院工学研究科）

本日の講演

- はじめに（導入）
  - 身近な暗号
  - そして重要な社会インフラである暗号！？
- 暗号とは何か？
  - 理解されていない暗号！
    - 知っているようで知らない！
    - 古典暗号と現代暗号
- 公開鍵暗号とは
  - デジタル世界の基盤
    - これが無ければ、世界は成り立たない！！

エニグマ(Enigma)

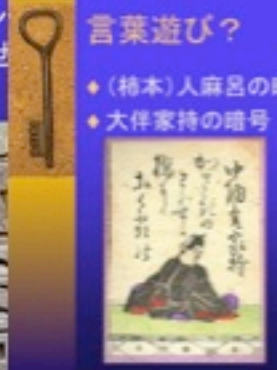
- 第二次世界大戦時のドイツ軍の暗号

多表式換字暗号

- レオン・バッティスタ・アルベルティ（15世紀）
- ジョヴァンニ・ボルタ（16世紀）
- ブレーズ・ド・ヴィジュネル（16世紀）
  - ヴィジュネル暗号
    - 周期的に換字表を変更

解読という意味；言語学やDNA等

- ロゼッタストーン
  - 1799年
  - ヒエログリフの解読
    - シャポリオンリエから見せった？



言葉遊び？

- （柿本）人麻呂の暗号
- 大伴家持の暗号

エドガー・アラン・ポー

- 黄金虫（1843）
  - 53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?34;48)4+;161;:188;+?;

ty-one degrees and seventh limb east -line from the tree

コナン・ドイル

- シャーロックホームズ：踊る人形

ビエト（記号代数学の父、数学者）

- 16世紀
  - スペインの暗号を解読
- ジョン・ウォリス
  - ∞
  - 暗号学者？
  - 鍵を使った暗号の構築？

安全・安心な暗号であるために

- 暗号アルゴリズムの公開性
  - 安全性の評価
    - 広く安全性に対して議論して
  - 暗号アルゴリズムを隠すこ
    - RC4の例が示すように
  - トラップドアの排除
    - 開発者が暗号に対して「仕
  - そして，広く利用されるため
    - 商用暗号の必要性
      - 安全・安心の上に，低いコスト

オイラーの定理

- フェルマーの小定理

$$a^{p-1} \equiv 1 \mod p$$

- オイラーの定理

$$a^{\varphi(n)} \equiv 1 \mod n$$

$\varphi(n)$ はオイラー関数。nと互いに素な数の個数

$n = pq$ でpとqが素数の場合

$$\varphi(pq) = (p-1)(q-1)$$

鍵交換アルゴリズムは、数学で作るテレパシー！？

$Y_a = z^{X_a} \mod p$

$Y_b = z^{X_b} \mod p$

X_b は秘密！

Y_a Y_b Y_a Y_b

$K_b = Y_a^{X_b} \mod p$

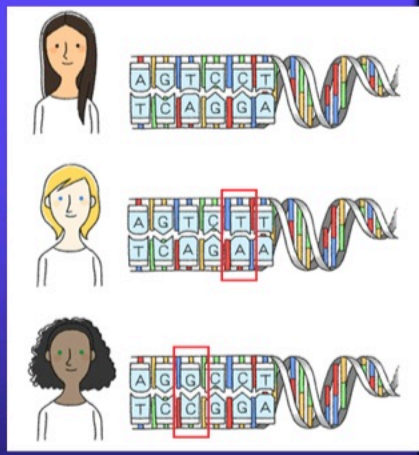
Y_b ? Y_a ?

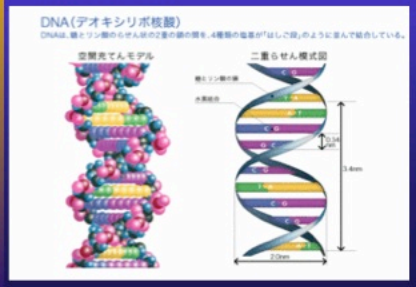
解読という意味；言語学やDNA等

- ロゼッタストーン
  - 1799年
  - ヒエログリフの解読
    - シャポリオンはフーリエから見せてもらった？

解読という意味；言語学やDNA等

- DNA
  - 塩基配列の解読
    - アデニン (A)、グアニン (G)、チミン (T)、シトシン (C)



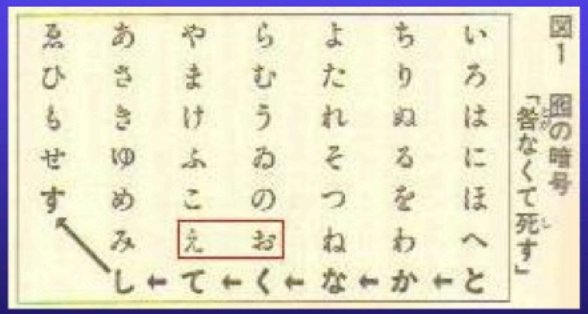


言葉遊び？

- （柿本）人麻呂の暗号
- 大伴家持の暗号

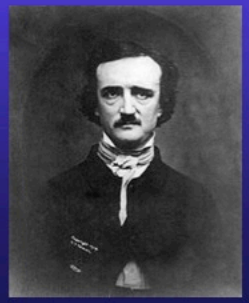
言葉遊び？

- いろは歌
  - 咎（罪）なくて死す



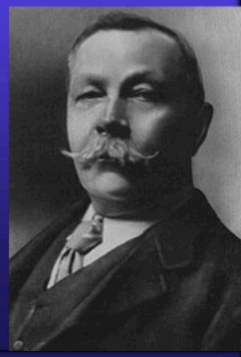
エドガー・アラン・ポー

- 黄金虫（1843）
  - 53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?34;48)4+;161;:188;+?;
  - A good glass in the bishop's hostel in the devil's --twenty-one degrees and thirteen minutes --northeast and by north --main branch seventh limb east side --shoot from the left eye of the death's-head --abee-line from the tree through the shot fifty feet out.
- 換字暗号
  - 文字を置き換える



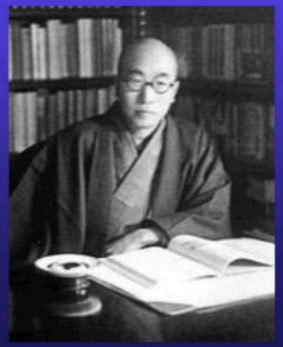
コナン・ドイル

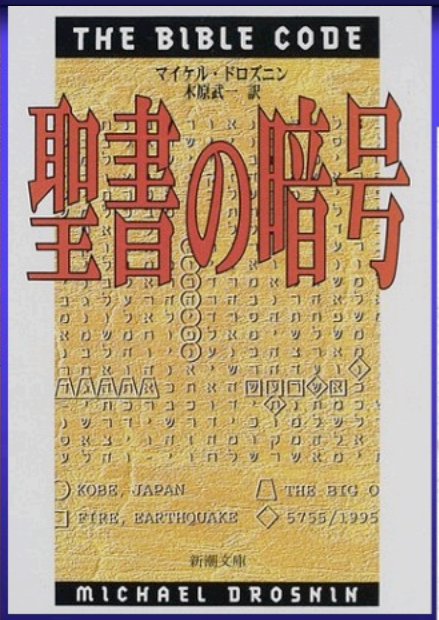
- シャーロックホームズ；踊る人形

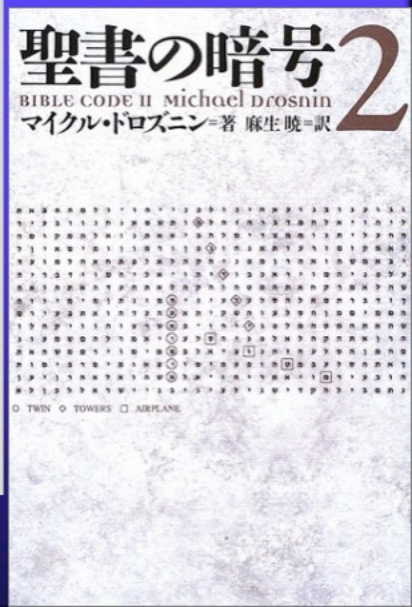


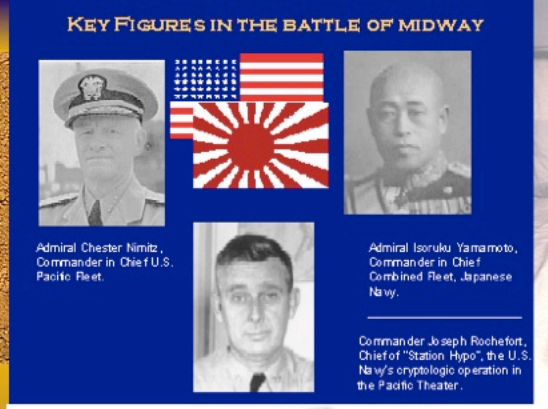
江戸川乱歩

- 二銭銅貨（1923）
  - 南無阿、南無弥陀仏、阿陀仏、陀、無阿弥陀、南弥、南仏









知られていない暗号の世界
ー実は身近に溢れている暗号とその仕組みー

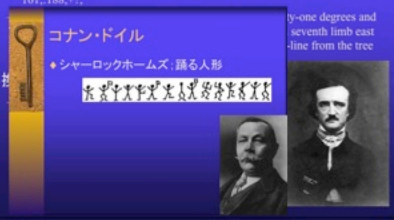
千里ライフサイエンスフォーラム
2012年12月20日
森井昌克
morii@ieee.org
（神戸大学大学院工学研究科）

本日の講演

- はじめに（導入）
  - 身近な暗号
  - そして重要な社会インフラである暗号！？
- 暗号とは何か？
  - 理解されていない暗号！
    - 知っているようで知らない！
    - 古典暗号と現代暗号
- 公開鍵暗号とは
  - デジタル世界の基盤
    - これが無ければ、世界は成り立たない！！

エドガー・アラン・ポー

- 黄金虫（1843）
  - 53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*;4069285);)6!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?34;48)4+;161;:188;+?;



ビエト（記号代数学の父、数学者）

- 16世紀
  - スペインの暗号を解読
- ジョン・ウォリス
  - ∞
  - 暗号学者？
  - 鍵を使った暗号の構築？

エニグマ(Enigma)

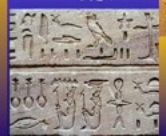
- 第二次世界大戦時のドイツ軍の暗号

多表式換字暗号

- レオン・バッティスタ・アルベルティ（15世紀）
- ジョヴァンニ・ポルタ（16世紀）
- ブレーズ・ド・ヴィジュネル（16世紀）
  - ヴィジュネル暗号
    - 周期的に換字表を変更

解読という意味；言語学やDNA等

- ロゼッタストーン
  - 1799年
  - ヒエログリフの解読
    - シャポリオンリエから見せった？



言葉遊び？

- （格本）人麻呂の暗号
- 大伴家持の暗号

安全・安心な暗号であるために

- 暗号アルゴリズムの公開性
  - 安全性の評価
    - 広く安全性に対して議論して
  - 暗号アルゴリズムを隠すこ
    - RC4の例が示すように
  - トラップドアの排除
    - 開発者が暗号に対して「仕
  - そして，広く利用されるため
    - 商用暗号の必要性
      - 安全・安心の上に，低いコス

オイラーの定理

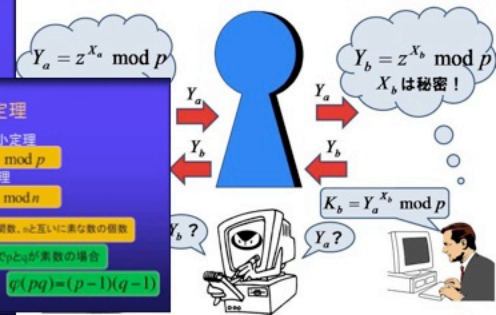
- フェルマーの小定理
  $a^{p-1} \equiv 1 \mod p$
- オイラーの定理
  $a^{\varphi(n)} \equiv 1 \mod n$

$\varphi(n)$ はオイラー関数，nと互いに素な数の個数

$n = pq$ でpとqが素数の場合

$\varphi(pq) = (p-1)(q-1)$

鍵交換アルゴリズムは、数学で作るテレパシー！？



身近な暗号

- ICOCA とPiTaPa

ＩＣ乗車券:相互利用、来年３月２３日から開始

毎日新聞　2012年12月18日　22時30分

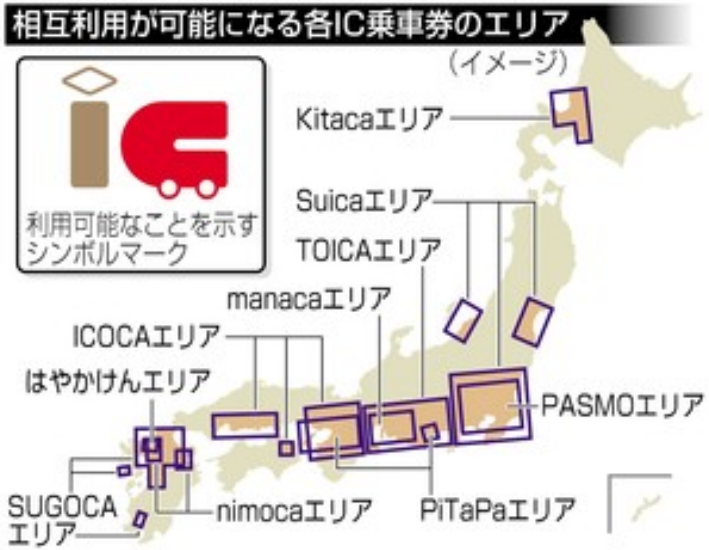
ＪＲ５社と全国の大手私鉄などは１８日、各社が発行する計１０種類のＩＣ乗車券について、来年３月２３日から相互利用を開始すると発表した。１枚のＩＣカードで、鉄道５２事業者、バス９６事業者の運賃が払えるようになる。

相互利用できるＩＣ乗車券は、ＪＲ西日本の「ＩＣＯＣＡ（イコカ）」、ＪＲ東日本の「Ｓｕｉｃａ（スイカ）」、関西私鉄の「ＰｉＴａＰａ（ピタパ）」、地下鉄を含む首都圏の「ＰＡＳＭＯ（パスモ）」など。１０種類合わせて計約８０００万枚が発行されており、相互利用できる枚数では世界最大規模となる。ただし、ＪＲ西日本管内で乗車してＪＲ東海の管内で下車するなど、エリアをまたいだ利用はできない。

ＪＲ西日本のＩＣＯＣＡはこれまで、ＳｕｉｃａなどＪＲ系３カードとＰｉＴａＰａのエリアで使用可能だった。またＰｉＴａＰａはこれまで、ＪＲ系では西日本のＩＣＯＣＡとだけ提携していた。【安藤大介】

身近な暗号

- ICOCA とPiTaPa



ＩＣ乗車券:相互利用、来年３月２３日から開始

毎日新聞　2012年12月18日　22時30分

ＪＲ５社と全国の大手私鉄などは１８日、各社が発行する計１０種類のＩＣ乗車券について、来年３月２３日から相互利用を開始すると発表した。１枚のＩＣカードで、鉄道５２事業者、バス９６事業者の運賃が払えるようになる。

相互利用できるＩＣ乗車券は、ＪＲ西日本の「ＩＣＯＣＡ（イコカ）」、ＪＲ東日本の「Ｓｕｉｃａ（スイカ）」、関西私鉄の「ＰｉＴａＰａ（ピタパ）」、地下鉄を含む首都圏の「ＰＡＳＭＯ（パスモ）」など。１０種類合わせて計約８０００万枚が発行されており、相互利用できる枚数では世界最大規模となる。ただし、ＪＲ西日本管内で乗車してＪＲ東海の管内で下車するなど、エリアをまたいだ利用はできない。

ＪＲ西日本のＩＣＯＣＡはこれまで、ＳｕｉｃａなどＪＲ系３カードとＰｉＴａＰａのエリアで使用可能だった。またＰｉＴａＰａはこれまで、ＪＲ系では西日本のＩＣＯＣＡとだけ提携していた。【安藤大介】

身近な

- ICOCA とPiTaPa
  - FeliCa
    - ソニー製の非接触ICカード
      - リーダ／ライタが市販されていて読込書込可能
  - 一部のデータは読める！？
    - いつ利用したかという履歴は見れる！
  - 暗号モードが存在する
    - 読込書込はできない！
    - IDAは偽造出来る？？

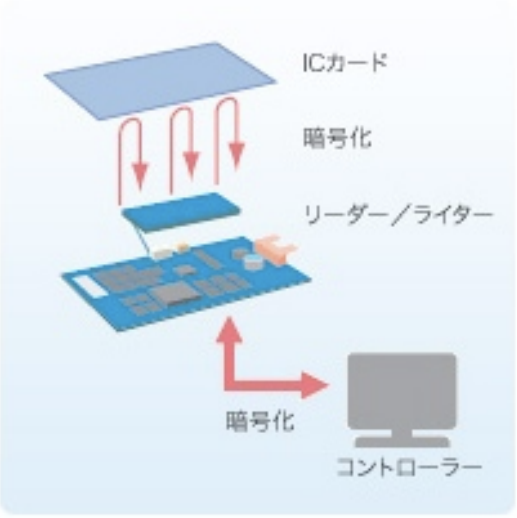
身近な暗号

- ICOCA とPiTaPa

6 セキュリティー

相互認証と通信データの暗号化においては、オープンスタンダードなセキュリティーアルゴリズムを採用し、信頼性の高いセキュリティーを実現しています。また、通信データの暗号鍵は相互認証ごとに新しく生成され、成りすましを防いでいます。

このような通信時のセキュリティーに加えて、カード発行時には発行者とカード製造会社との間で発行情報と鍵変更情報を暗号化した状態で安全に受け渡す独自の仕組みを提供しています。また、カード出荷時には「出荷鍵」を設定することにより、カード輸送から発行までの安全性を確保しています。



身近な暗号

- ICOCA とPiTaPa
- その他、ネット社会（デジタル社会）のどこでも何でも
  - 情報を守るための最後の砦；暗号
  - そして
    - （狭い意味の）暗号だけでなく、印鑑や書名のかわりも。
      - 私が私である事を保証してくれる「暗号」
      - ネット社会の身分証明書
        - » パスワードや身分証明者では守れない

NHK(2009年4月15日）

NHKニュース（2010年４月17日）

暗号とは

- 暗号を数式で表すと

  共通鍵暗号

$$C = f(K, M)$$

$$M = f^{-1}(K, C)$$

Mは平文（メッセージ）、Cは暗号文、Kは鍵、fは暗号化関数、f^{-1}は符号関数

簡単に言い換えれば！

暗号とは

- 小さな秘密(K)で大きな秘密(M)を守る事！
  - 小さな秘密(手持ちの風呂敷)で大きな秘密(大事な書類、持ち物)を覆ってしまう。
  - 小さな秘密(K)は大事！
  - パスワード(暗証番号)はその一例
    - 小さな秘密(パスワード)で大事なもの(銀行口座の全財産など)を守る

$$C = f(K, M)$$

$$M = f^{-1}(K, C)$$

暗号を使うためには

- 小さな秘密を相手（信頼出来る）と持ち合わなければ、暗号が使えない
  - 風呂敷の包み方（K）を相手が知らなければ、相手が風呂敷を解けない！！

相手に小さな秘密（K）を届ける
（小さな秘密を共有しないと行けない）

鍵共有

- 互いに秘密の鍵を持っておく必要が有る

  共通鍵暗号

$$C = f(K, M)$$

$$M = f^{-1}(K, C)$$

  - 安全な通信路を用いて、予め送る？
    - 大きな矛盾

鍵共有をどう実現する

- テレパシーができれば… 実現？
  - 相手にテレパシーで小さな秘密を送る事が出来れば、誰にも知られずに秘密を共有

でも、テレパシー？

同時に「同じ秘密」を思いつく事が出来れば！
（他の人は思いつかない！）

鍵共有をどうする？

- 数学で実現する
  - 数学トリックを使う
    - A（暗号化側）とB（復号側）だけがある数字を思いつく
    - 他の人は絶対に思いつかない
      - 正確には確率的に思いつかない
  - 離散対数問題を利用する
    - ちょっと難しいですが…　そんなものがあると思って

鍵共有を実現する

- Diffee-Hellman（DH）法
  - 離散対数問題を利用
  - 一方向性関数

$$y = g^a \bmod p$$

  - 易しい問題！
    - gとpとaを与えて、yを計算
  - 難しい問題！
    - gとpとyを与えて、aを計算

鍵交換アルゴリズムは、数学で作るテレパシー！？

$Y_a = z^{X_a} \bmod p$

X_a は秘密！

$Y_b = z^{X_b} \bmod p$

X_b は秘密！

Y_a

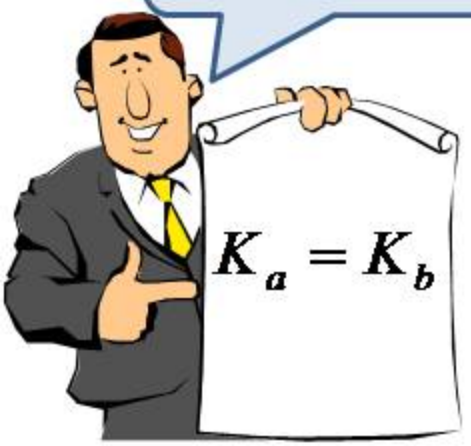
Y_b

Y_a

Y_b

$K_a = Y_b^{X_a} \bmod p$

$K_b = Y_a^{X_b} \bmod p$



Y_b ?

Y_a ?

今回のまとめ

速算術
カードマジック
テレパシーと暗号