サイエンス・パートナーシップ・プロジェクト

白と黒の符号・暗号理論

第１日　暗号理論の歴史

2012年8月30日

高知大学 理学部 応用理学科
情報科学コース　　塩 田 研 一

目　次

- 暗号とは
- 文字のなかった時代の暗号
- 文章の暗号化
  ― 換字式暗号と転置式暗号 ―
- 頻度解析による暗号解析法の発明
- 暗号機の登場
- コンピュータの登場
- インターネットの普及

暗 号 と は

- 暗号技術とは
  - 仲間にはわかるが
  - 仲間以外にはわからない

  ように、情報を加工して
  - 伝達したり
  - 保存したり

  する技術

文字のなかった時代の暗号

- 可能な情報伝達手段
  - 話し言葉
  - 絵
- 話し言葉における暗号
  - 符丁（隠語）
- 絵は暗号になるかな？

文字の発明

- 表意文字
  - 漢字　etc.
- 表音文字
  - ひらがな、カタカナ、アルファベット　etc.
- 文字の種類の多いのはどっち？
- 暗号を作り易いのはどっち？

シーザー暗号

- アルファベットで書いた文章の暗号化
- 各アルファベットを、3つ先のアルファベットに変換
- a, b, c, ... , w, x, y, z

D, E, F, ... , Z, A, B, C

問題です

- DSSOH = apple
- EDQDQD = banana
- FKHUUB = cherry

シーザー暗号の鍵

- 鍵:「3つ先」の「3」
- 鍵を「5」にすると
  - apple → FUUQJ
  - banana → GFSFSF
- 鍵を「10」にすると
  - apple → KZZVO
  - banana → LKXKXK

シーザー暗号は解き易い

- 鍵は25通りだけ
  （「0」では暗号にならないないから）

  ➡ 25通り全て試せば
  必ず当たる

- デモ

換字(かえじ)式暗号

- シーザー暗号のように
  文字の対応表
  を作って文字を変換する暗号
- アルファベット26文字なら鍵は何通り？
  26！= 403291461126605635584000000（27桁）
- デモ

Q & A

ご質問、ご意見ありましたら

転置式暗号

- アナグラムのように、
  文字の場所を入れ替える暗号

- アナグラム：
  さんばしどおり
  → おしどりさんば
  さばおりしんど　etc.

スキュタレー

- 転置式暗号の一種
- 棒に巻きつけた皮ひもに文章を書く
- ほどくと読めない
- 同じ太さの棒に巻きつければ読める

転置式ブロック暗号

- 例:「鍵」が順列 45213 の場合
  - 5文字をひとブロックとして処理
  - 5つの文字を
    1番目の文字を4番目に,
    2番目の文字を5番に, ...
    と並べ替える
  - apple → LPEAP
  - banana → ANNBA□□□A□
- デモ

中間まとめ

- 基本的に暗号の作り方は2つ
  - 換字式暗号
  - 転置暗号
- 換字式暗号の「鍵」の個数は膨大

  ➡ 第3者が「鍵」を知るのは不可能と思われていた

Q & A

ご質問、ご意見ありましたら

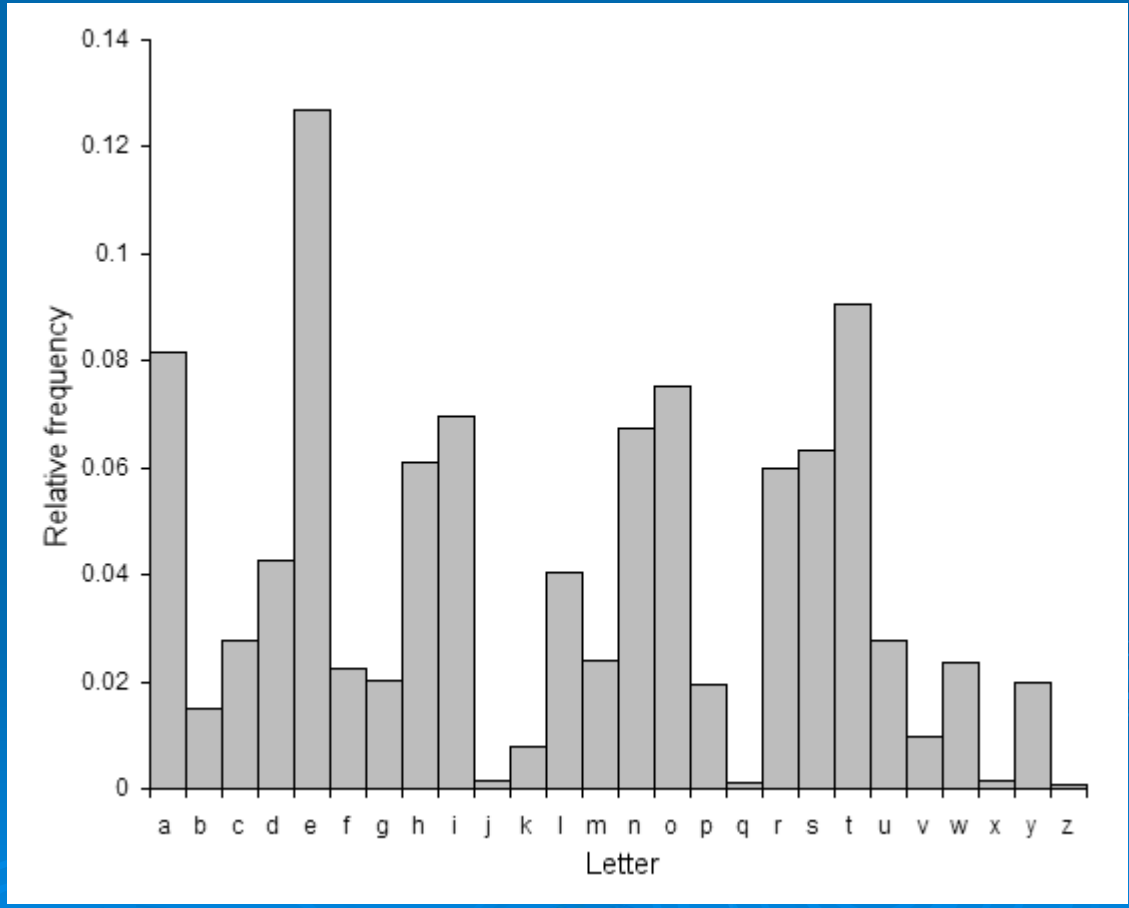
頻度解析による暗号解読

- ９世紀頃アラビアで発見？
- １６世紀頃にはヨーロッパに
- 各アルファベットの出現率の「ばらつき」に着目

以下、英語の場合で説明

頻度解析による暗号解読

英語の文章で
各アルファベットの出現率を
調べると …



頻度解析による暗号解読

- 換字式暗号では
  - １番多く現れる文字は e らしい,
  - ２番目に多く現れる文字は t らしい, ...
- その他のヒント
  - １文字単語は a と i のみ
  - よく使う2文字単語は of, to, in etc.
  - ２つ続く文字は ss, ee, tt, ff, ll, mm, oo etc.

➡ これでほとんど読めてしまう。

ヴィジュネル暗号

- ヴィジュネル方陣を「鍵」とする、より複雑な換字式暗号
- １６世紀に確立
- 永らく解読不可能と思われていた
- １９世紀に解析法発見
- 以後しばらく、強力な暗号が不在

無線通信の発明から第一次世界大戦

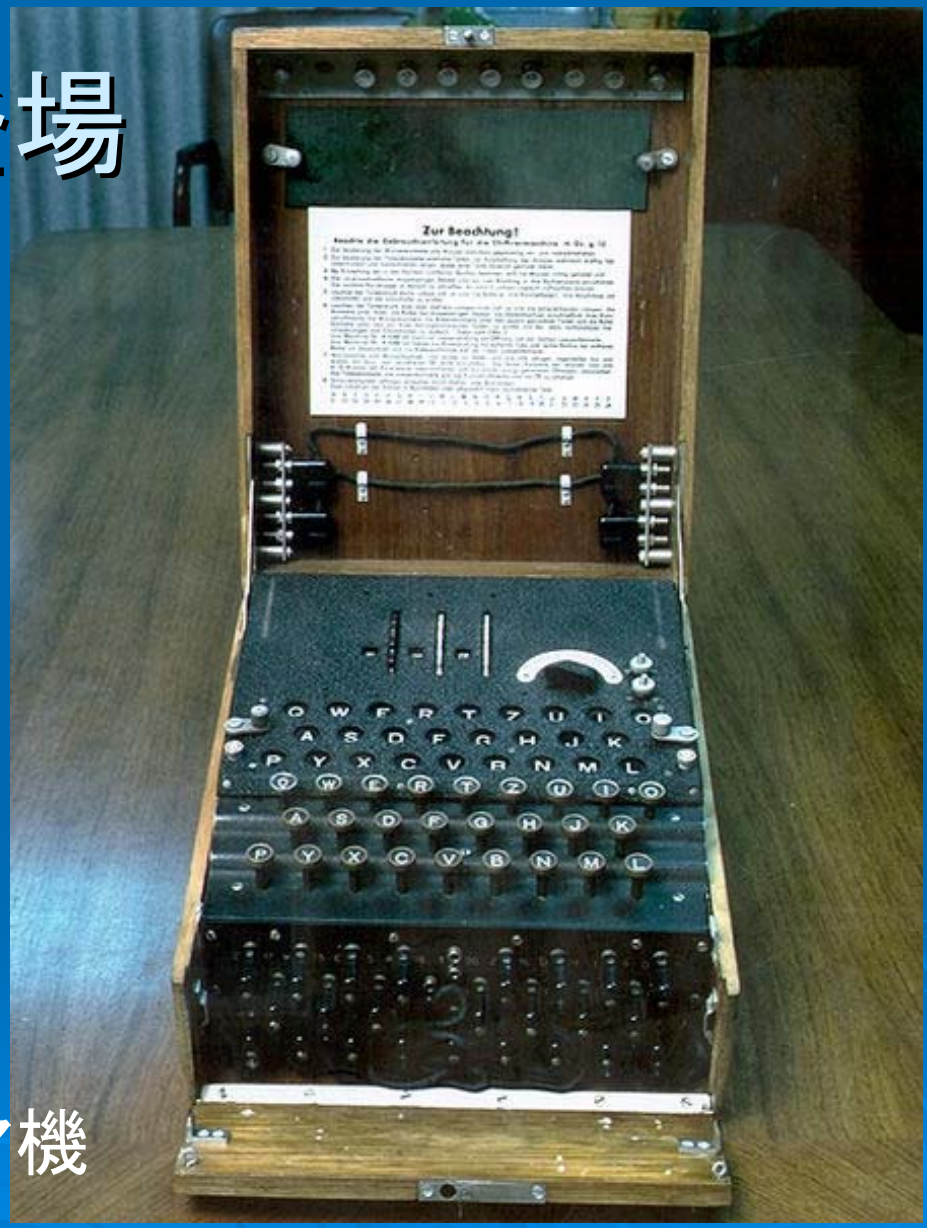
- 1901年大西洋無線横断実験成功
- 第1次世界大戦で活用
  - ただし暗号化が必須
- ドイツ軍はADFGVX暗号で優位に
  - 換字式と転置式の合せ技
- 暗号を破ってから連合国軍が形勢逆転

暗号機の登場

機械の登場により

- より複雑な変換
- 高速処理

が可能に



エニグマ機

第二次世界大戦
― エニグマをめぐる攻防 ―

- ドイツ軍は最強
  - エニグマで暗号通信
  - 神出鬼没のUボート
- フランスがスパイからエニグマの設計書入手（でも解析できず）
- 存続の危機にあったポーランドが解析法開発
- イギリスはエニグマ解析機ボンブを発明（ある意味、世界初のコンピュータ）

コンピュータの登場

- より高速な処理
- 文字単位の変換から数値の変換へ
  - 文字も、音声も、画像も全て2進データ
    - ➡ 様々なデータが暗号化可能に
- デモ
- 暗号解析もコンピュータで

インターネットの普及

- ネット上ではデータは誰でも傍受可能
- やりたいことは沢山
  - ネットショッピング
  - ネットバンキング
  - オンライン投票　etc.
- 暗号は必須

共通鍵暗号

- 暗号の送信者と受信者が同じ「鍵」を使用
- 1976年までは全ての暗号が共通鍵方式
- ネット時代では不都合が
  - 相手ごとに違う「鍵」が必要
  - 「鍵」はネットでは送れない

➡ 「鍵」の配送コストが膨大に

Q & A

ご質問、ご意見ありましたら

ま と め

- 暗号を進化させる要因
  - 暗号作成法と暗号解析法の相互作用
  - 機械の発明
  - コンピュータの発明
- 現在の状況
  - 暗号は日常生活の中に
  - 様々なデータが暗号化可能
  - 高度なセキュリティ

Q & A

ご質問、ご意見ありましたら

換字式暗号の「鍵」の作り方

- 「鍵」の簡単な作り方
  1. キーワードを決める
  2. キーワードを先頭に置き
  3. 他の文字は順番に後ろに続ける

- 例:
  - キーワード = ORANGE
  - 対応表 = ORANGEBCDFHIJK ...

認　証

- 認証も暗号技術のひとつ
- 実社会では
  - 本人であることの証明：印鑑、署名
  - 仲間であることの証明：合言葉

電子的に実現