現代暗号

～ネット社会の情報を守る暗号技術とは～

国立情報学研究所
渡辺　曜大

話の概要

- 暗号の使い道
- 暗号の歴史
  - 古典暗号:シーザー暗号，単一換字暗号の作り方，解き方
- 現代暗号
  - 公開鍵暗号，共通鍵暗号，量子暗号
  - 安全性とその証明

暗号の使い道

- 暗号というと…
  - スパイ
  - 戦争
  - 推理小説の名探偵

  ＊まっとうな人間には関係ない？
- 意外と身近なところで使われている
  - キーワード:「プライバシー」と「決済」

暗号の使い道

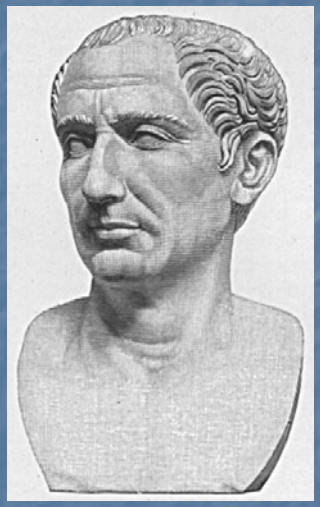
- インターネットで　　http:// ⇒ https://
  - 買い物
  - 情報（パスワード，クレジットカード番号，個人情報）入力
- 無線LAN
- ETC (Electric Toll Collection) システム
- ICキャッシュカード，ICクレジットカード
- おサイフケータイ

暗号の歴史

- 2000年以上の歴史　シーザー暗号（紀元前）
- 1970年代以前（古典暗号）
  - 軍事外交用途の非公開技術
  - 参加者限定の1対1通信を前提
- 1970年代以降（現代暗号）
  1976年 米国政府標準暗号DES制定と仕様公開
  1976,77年 公開鍵暗号の概念提唱・発明
  - 情報保護を目的とする公開技術
  - 不特定多数の参加者によるネットワーク通信

簡単な暗号：シーザー暗号

- ジュリアス・シーザー（Julius Caesar）



Wikipedia

B.C.100/7/13 – B.C.44/3/15

古代ローマ（共和政ローマ）の政治家で軍事的指導者．文筆家としても有名．

シーザー暗号

- 暗号作成
  3文字シフト

JULIUS CAESAR
↓
KVMJVT DBFTBS
↓
LWNKWU ECGUCT
↓
MXOLXV FDHVDU

- メッセージ復元
  3文字逆シフト

MXOLXV FDHVDU
↓
LWNKWU ECGUCT
↓
KVMJVT DBFTBS
↓
JULIUS CAESAR

暗号の基本的な用語

- 平文:伝えようとしているメッセージ
- 暗号化:第三者に分からないように平文を変換すること
- 暗号文:平文を暗号化したもの
- 復号:暗号文から平文を復元すること

暗号化・復号について

- 計算方式（アルゴリズム）と鍵を分けて考える
- シーザー暗号の場合
  - 暗号化
    アルゴリズム：n文字すすめる
    鍵：n=3
  - 復号
    アルゴリズム：n文字もどす
    鍵：n=3

シーザー暗号は安全か？

- 現代暗号の立場
  アルゴリズム公開のもとで安全性を検証する
- すなわち，暗号の安全性を考えるときアルゴリズムは既知と仮定する
- シーザー暗号であることが分かっていると…
  鍵を高々26通り調べてやれば解ける
  ⇒ シーザー暗号は安全ではない

単一換字暗号

- シーザー暗号

変換表

平文	ABCDEFGHIJKLMNOPQRSTUVWXYZ
暗号文	DEFGHIJKLMNOPQRSTUVWXYZABC

- 変換表をランダムに

平文	ABCDEFGHIJKLMNOPQRSTUVWXYZ
暗号文	MIOGAFYPHKUJLVCZESBRWTDNQX

⇒ 単一換字暗号

単一換字暗号

- 暗号化

  THIS IS A PEN ⟶ FKJI JI Y WCV

- 復号

  FKJI JI Y WCV ⟶ THIS IS A PEN

平文	ABCDEFGHIJKLMNOPQRSTUVWXYZ
暗号文	YARDCEHKJUNZLVSWXTIFGPOBMQ

単一換字暗号は安全か？

- 全数探索
  鍵（変換表）についてすべての起こりうる場合を調べる
  26!＝403291461126605635584000000通り
  ＊京速：10000000000000000(10P)演算/秒
  ＊1年＝365×24×60×60秒＝31536000秒
  1000年以上かかる　⇒ 非常に効率が悪い
- しかし，統計的手法（頻度分析）は有効

統計的手法：頻度分析

- 英文における文字の出現頻度に関する統計を利用
- 一般に英文が長いほど精度が高くなる
  - 一文字：ETAOINSHRDLUCMWFGYPBVKJXQZ
  - 二文字：TH HE IN ER AN RE ON AT EN ND
  - 三文字：THE AND ING ION ENT TIO
  - 単語：THE OF AND TO A IN AT IS I

出現頻度高 ←

注）サンプルによっては大きく外れる場合もある
『消失』ジョルジュ・ペレック著，ギルバート・アデア訳
仏語・英語：200ページ，消失しているのは “e”

頻度分析

- 小説にも登場
  - 『黄金虫』エドガー・アラン・ポー
    暗号文：53‡‡†305))6*;4826)4‡. ...
  - 『踊る人形の謎』コナン・ドイル
    暗号文：  ...
  - ＊どちらも単一換字暗号
  - ＊頻度分析をベースに解読
- 古代文字の解読

単一換字暗号を解いてみる

OMN MYUIKSI HJIKI BKI GM CLSLULMGU YIHAIIG HJI AMKCU JBC HJIKI YIIG CLSLULMGU HJI HBUQ AMNTC JBSI YIIG WMFDBKBHLSITO IBUO LG UNWJ WBUI L UJMNTC JBSI WMFFIGWIC ALHJ B WMTTBHLMG BGC BGBTOULU MZ HJI UJMKHIK AMKCU BGC JBC B AMKC MZ B ULGVTI TIHHIK MWWNKKIC BU LU FMUH TLQITO B MK L ZMK IPBFDTI L UJMNTC JBSI WMGULCIKIC HJI UMTNHLMG BUUNKIC YNH HJIKI YILGV GM CLSLULMGU FO ZLKUH UHID ABU HM BUWIKHBLG HJI DKICMFLGBGH TIHHIKU BU AITT BU HJI TIBUH ZKIXNIGH

- 言語:英語，暗号化:単一換字暗号

解読の手がかり

- 頻度分析
  暗号文中における文字の出現回数を数える
- 暗号文にスペースがあって単語の区切りが分かる ⇒ 短い語に注目
  - B, L: 一文字で出現
    a（不定冠詞） or I（一人称単数）？
  - HJI: 9回（内単語として6回）出現
    the, and, … ？

頻度分析

文字	A	B	C	D	E	F	G	H	I	J	K	L	M
出現回数	8	30	19	4	0	7	22	29	51	19	23	26	29
文字	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
出現回数	10	6	1	2	0	8	17	34	2	10	1	6	5

- I, U, B, H, M, ...の順
  ただちに
  I = e, U = t, B = a, H = o, M = I, ...
  とするのは短絡的
  ⇒ まず I = e を検証してみる

頻度分析:最頻出文字 “I” に注目

- “I”前後の文字の出現回数

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
前	2	0	1	0	0	1	0	4	3	9	9	0	0	1	0	0	1	0	5	5	2	0	2	0	4	0
後	0	2	5	1	0	0	5	3	3	0	9	1	0	0	0	1	0	0	0	3	0	0	0	1	0	0

AI:2回, IA:0回, BI:0回,IB:2回...

- 前後ともに出現O:E,M,O,R,V,Zの6文字のみ
  他の文字と相性がいい ⇒ 母音 （U:11文字）
- 連続出現 “II” が3回 ⇒ “ee”（or “oo”）

頻度分析:最頻出文字 “I” に注目

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
前	2	0	1	0	0	1	0	4	3	9	9	0	0	1	0	0	1	0	5	5	2	0	2	0	4	0
後	0	2	5	1	0	0	5	3	3	0	9	1	0	0	0	1	0	0	0	3	0	0	0	1	0	0

- J は前9後0, K は前9後9:J = h, K = r
  *二文字:th he in er an re
- HJI:9回出現: HJI = the
  *三文字:the and … *単語:the of …
- ちょうど HJIKI = there となる

暗号解読

OMN MYUerSe there Bre GM CLSLULMGU YetAeeG the AMrCU hBC there YeeG CLSLULMGU the tBUQ AMNTC hBSe YeeG WMFDBrBtLSeTO eBUO LG UNWh WBUe L UhMNTC hBSe WMFFeGWeC ALth B WMTTBtLMG BGC BGBTOULU MZ the UhMrter AMrCU BGC hBC B AMrC MZ B ULGVTe Tetter MWWNrreC BU LU FMUt TLQeTO B Mr L ZMr ePBFDTe L UhMNTC hBSe WMGULCereC the UMTNtLMG BUUNreC YNt there YeLGV GM CLSLULMGU FO ZLrUt UteD ABU tM BUWertBLG the DreCMFLGBGt TetterU BU AeTT BU the TeBUt ZreXNeGt

- Mr ⇒ or, M = o

暗号解読

OoN oYUerSe there Bre Go CLSLULoGU YetAeeG the AorCU hBC there YeeG CLSLULoGU the tBUQ AoNTC hBSe YeeG WoFDBrBtLSeTO eBUO LG UNWh WBUe L UhoNTC hBSe WoFFeGWeC ALth B WoTTBtLoG BGC BGBTOULU oZ the Uhorter AorCU BGC hBC B AorC oZ B ULGVTe Tetter oWWNrreC BU LU FoUt TLQeTO B or L Zor ePBFDTe L UhoNTC hBSe WoGULCereC the UoTNtLoG BUUNreC YNt there YeLGV Go CLSLULoGU FO ZLrUt UteD ABU to BUWertBLG the DreCoFLGBGt TetterU BU AeTT BU the TeBUt ZreXNeGt

- Bre ⇒ are, B = a, L = i

暗号解読

OoN oYUerSe there are Go CiSiUioGU YetAeeG the AorCU haC there YeeG CiSiUioGU the taUQ AoNTC haSe YeeG WoFDaratiSeTO eaUO iG UNWh WaUe i UhoNTC haSe WoFFeGWeC Aith a WoTTatioG aGC aGaTOUiU oZ the Uhorter AorCU aGC haC a AorC oZ a UiGVTe Tetter oWWNrreC aU iU FoUt TiQeTO a or i Zor ePaFDTe i UhoNTC haSe WoGUiCereC the UoTNtioG aUUNreC YNt there YeiGV Go CiSiUioGU FO ZirUt UteD AaU to aUWertaiG the DreCoFiGaGt TetterU aU AeTT aU the TeaUt ZreXNeGt

- aU iU ⇒ as is, U = s

暗号解読

OoN oYserSe there are Go CiSisioGs YetAeeG the AorCs haC there YeeG CiSisioGs the tasQ AoNTC haSe YeeG WoFDaratiSeTO easO iG sNWh Wase i shoNTC haSe WoFFeGWeC Aith a WoTTatioG aGC aGaTOsis oZ the shorter AorCs aGC haC a AorC oZ a siGVTe Tetter oWWNrreC as is Fost TiQeTO a or i Zor ePaFDTe i shoNTC haSe WoGsiCereC the soTNtioG assNreC YNt there YeiGV Go CiSisioGs FO Zirst steD Aas to asWertaiG the DreCoFiGaGt Tetters as AeTT as the Teast ZreXNeGt

- Go, soTNtioG ⇒ no, soTNtion, G = n

暗号解読

OoN oYserSe there are no CiSisions YetAeen the AorCs haC there Yeen CiSisions the tasQ AoNTC haSe Yeen WoFDaratiSeTO easO in sNWh Wase i shoNTC haSe WoFFenWeC Aith a WoTTation anC anaTOsis oZ the shorter AorCs anC haC a AorC oZ a sinVTe Tetter oWWNrreC as is Fost TiQeTO a or i Zor ePaFDTe i shoNTC haSe WonsiCereC the soTNtion assNreC YNt there YeinV no CiSisions FO Zirst steD Aas to asWertain the DreCoFinant Tetters as AeTT as the Teast ZreXNent

- Zor ⇒ for, Z = f

暗号解読

OoN oYserSe there are no CiSisions YetAeen the AorCs haC there Yeen CiSisions the tasQ AoNTC haSe Yeen WoFDaratiSeTO easO in sNWh Wase i shoNTC haSe WoFFenWeC Aith a WoTTation anC anaTOsis of the shorter AorCs anC haC a AorC of a sinVTe Tetter oWWNrreC as is Fost TiQeTO a or i for ePaFDTe i shoNTC haSe WonsiCereC the soTNtion assNreC YNt there YeinV no CiSisions FO first steD Aas to asWertain the DreCoFinant Tetters as AeTT as the Teast freXNent

- oYserSe, haSe Yeen ⇒ observe, have been

  Y = b, S = v

暗号解読

OoN observe there are no Civisions betAeen the AorCs haC there been Civisions the tasQ AoNTC have been WoFDarativeTO easO in sNWh Wase i shoNTC have WoFFenWeC Aith a WoTTation anC anaTOsis of the shorter AorCs anC haC a AorC of a sinVTe Tetter oWWNrreC as is Fost TiQeTO a or i for ePaFDTe i shoNTC have WonsiCereC the soTNtion assNreC bNt there beinV no Civisions FO first steD Aas to asWertain the DreCoFinant Tetters as AeTT as the Teast freXNent

- Civisions, anC ⇒ divisions, and, C = d

暗号解読

OoN observe there are no divisions betAeen the Aords had there been divisions the tasQ AoNTd have been WoFDarativeTO easO in sNWh Wase i shoNTd have WoFFenWed Aith a WoTTation and anaTOsis of the shorter Aords and had a Aord of a sinVTe Tetter oWWNrred as is Fost TiQeTO a or i for ePaFDTe i shoNTd have Wonsidered the soTNtion assNred bNt there beinV no divisions FO first steD Aas to asWertain the DredoFinant Tetters as AeTT as the Teast freXNent

- betAeen ⇒ between, A = w

暗号解読

OoN observe there are no divisions between the words had there been divisions the tasQ woNTd have been WoFDarativeTO easO in sNWh Wase i shoNTd have WoFFenWed with a WoTTation and anaTOsis of the shorter words and had a word of a sinVTe Tetter oWWNrred as is Fost TiQeTO a or i for ePaFDTe i shoNTd have Wonsidered the soTNtion assNred bNt there beinV no divisions FO first steD was to asWertain the DredoFinant Tetters as weTT as the Teast freXNent

- as weTT as ⇒ as well as, T = l

暗号解読

OoN observe there are no divisions between the words had there been divisions the tasQ woNld have been WoFDarativelO easO in sNWh Wase i shoNld have WoFFenWed with a Wollation and analOsis of the shorter words and had a word of a sinVle letter oWWNrred as is Fost liQelO a or i for ePaFDle i shoNld have Wonsidered the solNtion assNred bNt there beinV no divisions FO first steD was to asWertain the DredoFinant letters as well as the least freXNent

- woNld, shoNld ⇒ would, should, N = u

暗号解読

Oou observe there are no divisions between the words had there been divisions the tasQ would have been WoFDarativelO easO in suWh Wase i should have WoFFenWed with a Wollation and analOsis of the shorter words and had a word of a sinVle letter oWWurred as is Fost liQelO a or i for ePaFDle i should have Wonsidered the solution assured but there beinV no divisions FO first steD was to asWertain the DredoFinant letters as well as the least freXuent

- in suWh Wase ⇒ in such case, W = c

暗号解読

0ou observe there are no divisions between the words had there been divisions the tasQ would have been coFDarativel0 eas0 in such case i should have coFFenced with a collation and anal0sis of the shorter words and had a word of a sinVle letter occurred as is Fost liQel0 a or i for ePaFDle i should have considered the solution assured but there beinV no divisions F0 first steD was to ascertain the DredoFinant letters as well as the least freXuent

- anal0sis ⇒ analysis, 0 = y

暗号解読

you observe there are no divisions between the words had there been divisions the tasQ would have been coFDaratively easy in such case i should have coFFenced with a collation and analysis of the shorter words and had a word of a sinVle letter occurred as is Fost liQely a or i for ePaFDle i should have considered the solution assured but there beinV no divisions Fy first steD was to ascertain the DredoFinant letters as well as the least freXuent

- Fost liQely ⇒ most likely, F = m, Q = k

暗号解読

you observe there are no divisions between the words had there been divisions the task would have been comDaratively easy in such case i should have commenced with a collation and analysis of the shorter words and had a word of a sinVle letter occurred as is most likely a or i for ePamDle i should have considered the solution assured but there beinV no divisions my first steD was to ascertain the Dredominant letters as well as the least freXuent

- comDaratively ⇒ comparatively, D = p

暗号解読

you observe there are no divisions between the words had there been divisions the task would have been comparatively easy in such case i should have commenced with a collation and analysis of the shorter words and had a word of a sinVle letter occurred as is most likely a or i for ePample i should have considered the solution assured but there beinV no divisions my first step was to ascertain the predominant letters as well as the least freXuent

- sinVle ⇒ single, V = g

暗号解読

you observe there are no divisions between the words had there been divisions the task would have been comparatively easy in such case i should have commenced with a collation and analysis of the shorter words and had a word of a single letter occurred as is most likely a or i for ePample i should have considered the solution assured but there being no divisions my first step was to ascertain the predominant letters as well as the least freXuent

- ePample ⇒ example, P = x

暗号解読

you observe there are no divisions between the words had there been divisions the task would have been comparatively easy in such case i should have commenced with a collation and analysis of the shorter words and had a word of a single letter occurred as is most likely a or i for example i should have considered the solution assured but there being no divisions my first step was to ascertain the predominant letters as well as the least freXuent

- freXuent ⇒ frequent, X = q

暗号解読

you observe there are no divisions between the words had there been divisions the task would have been comparatively easy in such case i should have commenced with a collation and analysis of the shorter words and had a word of a single letter occurred as is most likely a or i for example i should have considered the solution assured but there being no divisions my first step was to ascertain the predominant letters as well as the least frequent

- 完了!!

『黄金虫』エドガー・アラン・ポー

You observe there are no divisions between the words. Had there been divisions, the task would have been comparatively easy. In such case I should have commenced with a collation and analysis of the shorter words, and had a word of a single letter occurred, as is most likely, (a or I, for example,) I should have considered the solution assured. But, there being no divisions, my first step was to ascertain the predominant letters, as well as the least frequent.

- 登場人物が暗号解読について語る件

問題1

JV FKC WTCICVF RYIC JVDCCD JV YZZ RYICI SE ICRTCF OTJFJVH FKC EJTIF XGCIFJSV TCHYTDI FKC ZYVHGYHC SE FKC RJWKCT EST FKC WTJVRJWZCI SE ISZGFJSV IS EYT CIWCRJYZZM YI FKC LSTC IJLWZC RJWKCTI YTC RSVRCTVCD DCWCVD SV YVD YTC PYTJCD AM FKC HCVJGI SE FKC WYTFJRGZYT JDJSL JV HCVCTYZ FKCTC JI VS YZFCTVYFJPC AGF CBWCTJLCVF DJTCRFCD AM WTSAYAJZJFJCI SE CPCTM FSVHGC NVSOV FS KJL OKS YFFCLWFI FKC ISZGFJSV GVFJZ FKC FTGC SVC AC YFFYJVCD AGF OJFK FKC RJWKCT VSO ACESTC GI YZZ DJEEJRGZFM JI TCLSPCD AM FKC IJHVYFGTC FKC WGV SV FKC OSTD NJDD JI YWWTCRJYAZC JV VS SFKCT ZYVHGYHC FKYV CVHZJIK AGF EST FKJI RSVIJDCTYFJSV J IKSGZD KYPC ACHGV LM YFFCLWFI OJFK FKC IWYVJIK YVD ETCVRK YI FKC FSVHGCI JV OKJRK Y ICRTCF SE FKJI NJVD OSGZD LSIF VYFGTYZZM KYPC ACCV OTJFFCV AM Y WJTYFC SE FKC IWYVJIK LYJVYI JF OYI J YIIGLCD FKC RTMWFSHTYWK FS AC CVHZJIK

- 言語:英語, 暗号化:単一換字

問題2

RCGMQIQSMGHCMVGMJBCCVYHMVRPCMSGHVYBMSMIIHMVMGLHSMJVCRCSHCWBFCS
PHBJHVUBRCLMBCVSQMRSHCCFOMSGHVMJBMRSHCRCCCFHVBHYVHFHOMVRZCJHRH
OHMVBICWYPRMVGZMHGFCSIQMSHOPMVGOCSSWZRMVYJCOMVMGHMVIMVUHVYOCSZ
CSMRHCVHVFCSLWBMJJCFPCDCWSOCWVRSQVCDSHBUBGQHVYCFBRMSTMRHCVMSWL
CWSRPMRBLQHVHRHMJRPCWYPRMBHBDHROPCFFLQSMGHCMSWLCWSCSZCBBHIJQMP
CMNZSCZMYMVGMHLWSLWSMVNHCWBJQMBRPCWYPKWBRIQBMQHVYBCHLHYPRMJJMQ
LQGCWIRBRQZHOMJZCJHRHOHMVBZSCZMYMVGMIWRZWIJHOCZHVHCVYSMGWMJJQM
IBCSIBHRMBMFMORHVGHTHGWMJBBRMSRBRSWRRHVYMSCWVGDHRPBRCWROJWIBFC
CGYJCSHCWBFCCGHBMOCLLCVOSQCOOMBHCVMJJQBWVYRCIMSRBLWBHODHRPCSGH
VMSQPMSGDCSUHVYFCJUPMSMBBHVYCFFHOHMJBICRPJCOMJMVGVMRHCVMJMVGOW
SBHVYOMZHRMJHBRBMVGOMZRMHVBCFHVGWBRSQOCZBBPSHVUFSCLYCHVYCWRCVV
HYPRBPHFR

- 言語：英語，暗号化：単一換字
- ヒント：出現頻度の統計に大きな偏りがある

単一換字暗号の複雑化

- 頻度分析がなぜ有効か？
  暗号文の文字が同じならば平文の文字も同じだから
- 同音換字：1対多変換
- 多表式換字：複数の変換則
- 綴字換字：多対多変換
- 参考）転置暗号

古典暗号から現代暗号へ

- 設計が複雑化 ⇒ 解読も複雑化
  - 結局いたちごっこ
- 安全性の拠り所がほしい ⇒ 現代暗号
- 現代暗号の立場
  - 暗号方式（アルゴリズム）公開
  - 安全性証明

  ⇒ 第三者の安全性検証による信頼性向上

現代暗号における安全性

- 何をもって安全と考えるか？
  - 計算量的安全性
  - 情報量的安全性
- どうやって安全性を証明するか？
  - 計算量的安全性:ラビン暗号
  - 情報量的安全性:バーナム暗号

計算量的安全性

- 問題：n＝19048567を素因数分解せよ
  - 全数探索：小さい素数から順に割ってみる
    ⇒時間をかければ必ず解ける
    　桁数が大きくなると膨大な時間が必要
  - 全数探索“的”にしか解けないと考えられている
- 暗号が計算量的に安全であるとは
  - 暗号を破るには膨大な時間が必要で現実的に不可能

情報量的安全性

- 問題：1から10000までの数をランダムに選びましたこれを当ててください
  - どんなに時間をかけてもまぐれ当たり(確率0.0001)のみ
- 暗号が情報量的に安全であるとは
  - そもそも情報が不足していて暗号を破ることができない
  - 無限の計算資源をもつ攻撃者に対しても安全
    ⇒“無条件の安全性”とも呼ばれる
  - “事前に鍵（乱数）を共有していなければならない”というような強い仮定（制約）が必要

情報量的に安全な暗号の例

- 換字暗号において，“平文長＝鍵長”とすると
  ⇒ 1つの暗号文に対しすべての平文が候補に

暗号文	鍵	平文
KLXSCUHK	YARDCEHK	ILOVEYOU
KLXSCUHK	YWDBCEHK	IHATEYOU

鍵

A: 0文字シフト
B: 1文字シフト
C: 2文字シフト
…

- どちらの（あるいは第3，第4…の）平文が暗号化されたのかまったく分からない
  ⇒ 解読不可能
- アルファベット＝{0,1} ⇒ バーナム暗号

バーナム暗号

- 平文m，鍵s:{0,1}の列
- 鍵:完全にランダム(一様分布)
- 暗号化:$E_s(m)=m \oplus s$
- 復号:$D_s(c)=c \oplus s$
- $D_s(E_s(m))=s \oplus (m \oplus s)=m \oplus (s \oplus s)=m$

排他的論理和
0 ⊕ 0 = 0
0 ⊕ 1 = 1
1 ⊕ 0 = 1
1 ⊕ 1 = 0

暗号化	
平文	11001
鍵	⊕01101
暗号文	=10100

復号	
暗号文	10100
鍵	⊕01101
平文	=11001

情報量的安全性の証明(具体例)

- 1ビットバーナム暗号
- 攻撃者の平文に関する情報
  - 暗号文cを得る前:Pr[m=0], Pr[m=1]
  - 暗号文cを得た後:Pr[m=0|c=0], Pr[m=0|c=1]
- 暗号文cから情報が漏れないためには
  - 事前分布と事後分布が一致(mとcが独立)
    Pr[m=0|c=0]=Pr[m=0]
    Pr[m=0|c=1]=Pr[m=0]

1ビットバーナム暗号の安全性

- 事後確率の評価

$$\Pr[m=0 \mid c=0] = \frac{\Pr[m=0 \wedge c=0]}{\Pr[c=0]}$$

$$= \frac{\Pr[m=0]\Pr[s=0]}{\Pr[m=0]\Pr[s=0]+\Pr[m=1]\Pr[s=1]} = \Pr[m=0]$$

- Pr[m=0|c=1]=Pr[m=0]も同様に示すことができる
- 定理: バーナム暗号は完全秘匿性をもつ

共通鍵暗号と公開鍵暗号

- 共通鍵暗号：事前に何らかの方法により鍵を共有していなければならない
  - バーナム暗号：膨大な鍵が必要
    ⇒ コストが大きすぎる
    （米ロ大統領間の通信）
- 事前に鍵を共有せずに使える暗号はないか？
  ⇒ 公開鍵暗号

公開鍵暗号

- 共通鍵暗号 （対称暗号）
  暗号化用の鍵 ＝ 復号用の鍵
  鍵は秘密
- 公開鍵暗号 （非対称暗号）
  暗号化用の鍵 ≠ 復号用の鍵
  暗号化用の鍵:公開
  復号用の鍵:秘密

公開鍵暗号

- 1976年 ディフィー(Diffie)，ヘルマン(Hellman)によって公開鍵暗号の概念が提唱される
- 1977年 リベスト(Rivest)，シャミア(Shamir)，アドルマン(Adleman)によって公開鍵暗号（いわゆるRSA暗号）が発明される

公開鍵暗号の利点

- 暗号化用の鍵が公開されているので
  - 鍵管理が容易
    事前に･相手ごとに鍵を共有する必要なし
    不特定多数が参加するネットワーク
  - 誰でも暗号化できる
    秘密鍵を知らないとできない計算をさせて，
    その計算結果を公開鍵を使って検証

公開鍵暗号の実現

- 一方向性関数を使う
  - 一方向性関数とは？
    f(x)の計算は簡単
    逆関数の計算は難しい（時間がかかる）
  - 一方向性関数の例（候補）
    f(x,y)=x・y　逆関数は素因数分解に相当
- 計算量的安全性

素因数分解は本当に難しいか？

- 多くの研究者は素因数分解は難しい（多項式時間で解けない）と考えている
- 状況証拠
  - 人類が2000年以上かけても解けていない
  - RSA社の懸賞問題

桁数(bit)	576	640	704	768	896	1024	1536	2048
懸賞金($US)	10000	20000	30000	50000	75000	100000	150000	200000
解読状況	Dec03	Nov05	-	-	-	-	-	-

http://www.rsasecurity.com/rsalabs/node.asp?id=2093

一方向性関数の例（候補）

- 離散対数問題
  素数p，整数g,x,yに対して$g^x \bmod p = y$が成り立つことを $\log_g y \bmod p = x$ とあらわす
  ＊p,g,yから $x = \log_g y \bmod p$ を求める問題
- 剰余演算 （時計13時＝1時）
  a mod b: aをbで割った余り．bのことを法という
  例）17 mod 5 = 2,
  3 mod 11 = 3,
  -1 mod 7 = 6, …

離散対数問題

- 問題: $2^x \bmod 11=3$ なる x をもとめよ
- 全数探索により解くことができる

$2^1 \bmod 11=2$, $2^2 \bmod 11=4$, $2^3 \bmod 11=8$,…

x	0	1	2	3	4	5	6	7	8	9	10
y	1	2	4	8	5	10	9	7	3	6	1

- 表より x=8(+10k) が求める答え

平方剰余

- 素数p,qの積n=pqを法とする剰余計算を考える
- p=3,q=5として $f(x)=x^2 \bmod n$ を計算してみる

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
f	0	1	4	9	1	10	6	4	4	6	10	1	9	4	1

- 平方根 （ラビン暗号）
  - f(x)=1 を解くと x=1,4,11,14
- yがp,qと互いに素のときf(x)=f(y)をみたすxは4つ存在する

計算量的安全性を証明するために

- 暗号を破るのに最低限必要な計算量(計算時間)を見積もりたい
  - 計算量の下界を見積もるのは一般に非常に難しい
- 次善の策:暗号の安全性を，解くのが難しいと考えられている問題(例えば素因数分解)の困難性に帰着させる
  - 主張したいこと:問題Pが難しい ⇒ 暗号Cが安全
    対偶:暗号Cが安全でない ⇒ 問題Pが簡単
  - “暗号Cを破るアルゴリズムを用いて，問題Pを解くアルゴリズムを構成する”ことにより安全性を証明する

計算量的安全性の証明(具体例)

剩余演算

x mod n: xをnで割った余り

- ラビン暗号
  p, q:素数, n=pq
  公開鍵:n, 秘密鍵:p, q
  暗号化:$c=m^2 \bmod n$
  復号:$m=c^{1/2} \bmod n$
  （復号の一意性のため仕掛けが必要）
- 定理

素因数分解が難しければ，ラビン暗号は安全である
（暗号文から平文を求めるのは難しい）.

ラビン暗号の安全性証明

- 証明の概略:ラビン暗号の暗号文から平文を求めるアルゴリズムAを用いて，素因数分解アルゴリズムBを構成する.
  構成法:

B(n)

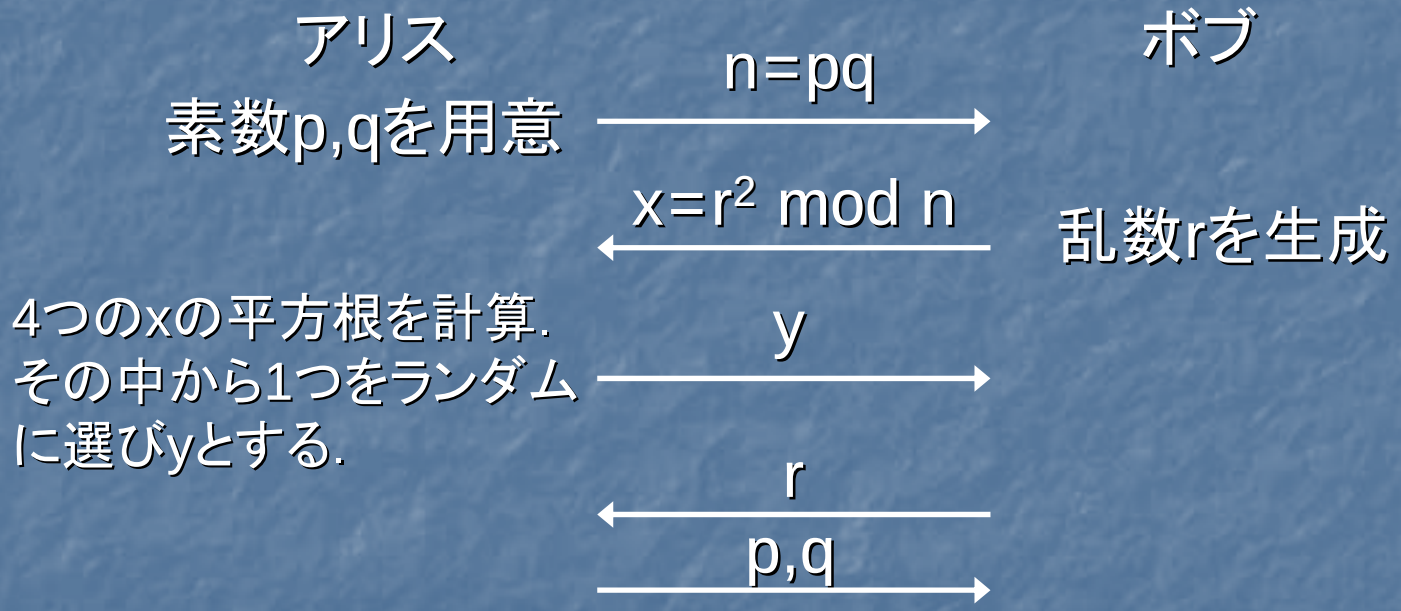
- もし，y≠±x (mod n)かつyがaの平方根になっているならば，GCD(x-y, n)=p or qである.
  ここで，aは4つの平方根をもち，xはランダムに選ばれているので，Pr[y≠±x (mod n)]=2/4=1/2.
  つまり，Bの成功確率はAの成功確率の1/2である.
  よって，素因数分解が難しければラビン暗号が安全であることが証明された.

暗号プロトコル：電話でジャンケン

- 状況設定：
  アリスとボブは電話でコイン投げがしたい．
  （二人はちょうど離婚して離れた町に住んでおり，どちらが車を所有するか決めようと思っている）
  M. Blum “Coin flipping by telephone”, 24th IEEE Compcon 1982 のAbstractより抜粋
- 公開鍵暗号のアイデアを使って解決
  - 追加設定：
    アリスとボブは素因数分解が難しいと信じている

電話でジャンケン

- 以下の手順で通信　（ラビン暗号が参考になる）



x＝±rならばアリスの勝ち

計算量的安全性の拠り所

- 計算量的問題の難しさ
  ある計算量的問題を解くことが難しければ，
  暗号を破ることができない
  - 例）ラビン暗号：素因数問題が難しければ安全
    RSA暗号：RSA問題が難しければ安全
- もっともらしい（できるだけ弱い）仮定のもとで
  安全性を証明することが重要
  - 効率性との兼ね合いが難しい

量子暗号

- ミクロの世界では，我々の日常的な直感に反するような現象が起こっている：
  不確定性原理，状態の重ね合わせ
- これらの現象を記述する力学：量子力学
  ⇔古典（ニュートン）力学
- 量子力学で記述されるような現象をうまく利用して，強力な（特に，情報量的に安全な）暗号を構成できないか？
- 量子力学に基づく新しい情報技術：量子情報技術
  - 量子コンピュータ，量子テレポーテーション，稠密符号化

量子暗号

- 量子ビットコミットメント
  - 安全なマルチパーティプロトコルの基礎となる暗号プロトコル
    ＊ビットコミットメント+量子通信路⇒紛失通信
  - “情報量的に安全な量子ビットコミットメントは存在しない”ことが証明されている
- 量子鍵配送
  - 2者間で秘密鍵(乱数)を共有するための技術
  - 情報量的に安全であることが証明されている

発表者の研究テーマ

- 量子暗号（量子鍵配送）の安全性
  - 現実の（必ずしも理想的とは限らない）装置を用いた場合でも安全な量子鍵配送の構成
- 暗号系（たとえば公開鍵暗号）の安全性概念の間に成り立つ関係

まとめ

- 暗号の歴史
  - 古典暗号:シーザー暗号，単一換字暗号
  - 頻度分析
- 現代暗号
  - 安全性
    計算量的安全性，情報量的安全性
  - 安全性証明
    ラビン暗号，バーナム暗号