符号理論･暗号理論

- No.12 共通鍵暗号 -

渡辺 裕

Coding Theory / Cryptography

- No.12 Common Key Crypt System -

Hiroshi Watanabe

共通鍵暗号方式

- 暗号化と復号に同じ鍵を用いる
  - 比較的高速に処理可能
  - 大容量データの転送に向く
  - 鍵の配送･管理に注意が必要
  - 配送先が増えると鍵の種類も増加
- 代表的な共通鍵暗号方式
  - DES (Data Encryption Standard), トリプルDES
  - FEAL
  - PGP
  - AES (Advanced Encryption Standard)
  - Camellia

Common Key Crypt System

- Same key is used for encryption and decryption
  - Relatively high speed
  - Suitable for large capacity transfer
  - Needs care for key delivery and management
  - The number key increases depends on the number of member
- Typical common key crypt system
  - DES (Data Encryption Standard), Triple DES
  - FEAL
  - IDEA
  - AES (Advanced Encryption Standard)
  - Camellia

DES (1)

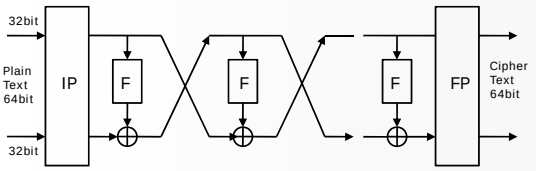
- 米国の旧暗号標準規格
  - 1976年国立標準局 (NBS) がアメリカ合衆国の公式連邦情報処理標準 (FIPS) として採用
  - 56ビットの鍵
  - 公募によりIBMの提案を採用
  - 均衡型Feistel構造
- ブロック暗号
  - 固定ビット長の平文を入力, 同じ長さの暗号文を出力
  - ブロック長64ビット(8ビットパリティ)
  - 16の処理工程(ラウンド)
  - Feistel構造: 32ビットずつ2分割され別の処理を施す

DES (1)

- US old encryption standard
  - NBS adopted as a federal information processing standard (FIPS) in 1976
  - 56 bit key
  - Adopt IBM proposal from public
  - Balanced Feistel structure
- Block cipher
  - Input fixed bit message, output same length crypt
  - Block length 64 bit (8 bit parity)
  - Round number: 16
  - Feistel structure: two separated 32 bit

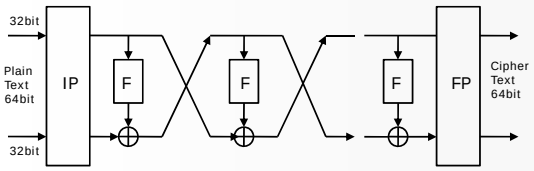
DES (2)

- 構造



DES (2)

- Feistel structure



DES (3)

- Feistel関数 (F関数)
  - Expansion: 32ビットを48ビットに拡張
  - Key mixing: 48ビットのラウンド鍵とExpansion出力のXOR
  - Substitution: 8個の6ビットから8個の4ビットをテーブル参照
  - Permutation: Substitution出力32ビットを並べ換え
- 鍵スケジュール
  - ラウンド鍵を生成
  - Permuted Choice 1 (PC-1): 64ビットから56ビットを抽出
  - Permuted Choice 2 (PC-2): PC1の半分から24ビット選択

DES (3)

- Feistel function (F function)
  - Expansion: 32 bit to 48 bit
  - Key mixing: XOR with 48 bit round key and Expansion output
  - Substitution: from 8x6 bit to 8x4 bit by table
  - Permutation: Substitution output by relocate 32 bit
- Key schedule
  - Generate round key
  - Permuted Choice 1 (PC-1): extract 56 bit from 64 bit
  - Permuted Choice 2 (PC-2):select 24 bit from half of PC1

DES (4)

- 総当たり攻撃
  - 鍵のとりうる値を全て試す方法
  - 1チップでの暗号化実現性から, 鍵長を56ビットに設定
  - 1999年には22時間で解読
- 高速攻撃法
  - 差分解読法 (2^{47})
    - 固定された差を持つ二つの平文の組を用い, 暗号文の組の差を計算し, その分布から統計的パターンを発見
  - 線形解読法(2^{43})
    - 暗号化変換の線形近似式を発見
  - Davies' attack (2^{50})
    - 経験的に分布を計算

DES (4)

- Brute force attack
  - Try all values of possible key
  - Set key length to 56 bit for implementation by 1chip
  - Could solve by 22 hours in 1999
- Fast attack
  - Differential cryptanalysis (2^{47})
    - Use fixed differential two messages, find stochastic pattern from distributions
  - Linear cryptanalysis(2^{43})
    - Find linear approximation for encryption
  - Davies' attack (2^{50})
    - Calculate empirical distribution

DES (5)

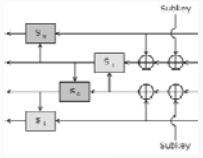
- トリプルDES
  - DESを鍵長を変えて3回繰り返す
    - C = encrypt$_{k3}$(decrypt$_{k2}$(encrypt$_{k1}$(P)))
    - P:平文
    - C:暗号文
    - ki:鍵
  - 鍵長は112ビット, 168ビット

DES (5)

- Triple DES
  - Repeat DES three times by changing key length
    - C = encrypt$_{k3}$(decrypt$_{k2}$(encrypt$_{k1}$(P)))
    - P: message
    - C: cryptgaph
    - ki: key
  - Key length are 112 bit, 168 bit

FEAL

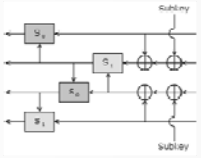
- FEAL (Fast data Encipherment Algorithm
  - ICカード等の8ビットマイクロプロセッサ上のソフトウェア向きに設計された暗号アルゴリズム
  - NTTが開発(1987), 64ビット, 128ビットの鍵を使用
  - FEAL-8は, DESよりも高速
  - FEAL-N/NX (N:段数, N:鍵長64ビット, NX:鍵長128ビット)
  - 現在はFEAL-32X
  - FEAL-32は2^{99}で解読可能



http://ja.wikipedia.org/wiki/FEAL

FEAL

- FEAL (Fast data Encipherment Algorithm
  - Designed for software implementation on 8 bit microprocessor such as IC card
  - Developed by NTT(1987), key length 64bit, 128 bit
  - FEAL-8 is fastger than DES
  - FEAL-N/NX (N:round, N: key length 64 bit, NX: long key length 128 bit)
  - Now FEAL-32X
  - FEAL-32 can be solved at 2^{99}



http://ja.wikipedia.org/wiki/FEAL

IDEA

- International Data Encryption Algorithm
  - メイル暗号化アプリケーション(PGP)で使用
  - James L. Massy, Xuejia Lai (1992)
  - ブロック長64ビット, 鍵長128ビット, 8ラウンド
  - 非商用利用については自由
  - 特許期限が2011年
- PGP (Pretty Good Privacy)
  - Philip Zimmermannが開発、公開した暗号ソフトウェア
  - PGP Corporation (2002), Symantec (2010)
  - Windows環境で電子メイルを暗号化

http://www.cla-ri.net/pgp/

IDEA

- International Data Encryption Algorithm
  - Used by mail encryption application (PGP)
  - James L. Massy, Xuejia Lai (1992)
  - Block length 64 bit, Key length 128 bit, 8 round
  - Free for non-commercial use
  - Patent expired in 2011
- PGP (Pretty Good Privacy)
  - Developed by Philip Zimmermann
  - PGP Corporation (2002), Symantec (2010)
  - E-mail is encrypted in Windows environment

http://www.cla-ri.net/pgp/

AES (1)

- AES (Advanced Encryption System)
  - 米国国立標準技術研究所(NIST)が公募
  - Rijndael (ラインダール) = フィンセント・ライメン (Vincent Rijmen) + ヨアン・ダーメン (Joan Daemen) (2000)
  - 鍵長は128ビット, 192ビット, 256ビット, ブロック長128ビット, ラウンド数10,12,14のSPN構造
  - 無線LANに応用 (WPA2)
  - 欧州暗号規格NESSIE, 日本暗号規格CRYPTRECで採用
- ラウンド
  - 8ビットを4x4行列に配置
  - 1ラウンドの操作は, SubBytes(), ShiftRows(), MixColumns(), AddRoundKey()

AES (1)

- AES (Advanced Encryption System)
  - NIST called for proposal
  - Rijndael = Vincent Rijmen + Joan Daemen (2000)
  - Key length 128, 192, 256 bit, block length 128 bit, round number 10, 12, 14 SPN structure
  - Applied to wireless LAN (WPA2)
  - European encryption standard NESSIE, Japanese encryption standard CRYPTREC
- round
  - 8 bit are placed to 4x4 matrix
  - 1ラウンドの操作は, SubBytes(), ShiftRows(), MixColumns(), AddRoundKey()

AES (2)

- 暗号化アルゴリズム
  - SubBytes(): 行列の要素である各1バイトでビット転置, x^8を最高次数とする多項式に対して逆元を計算し, 指定の行列でアフィン変換. S-Boxの転置処理に相当.
  - ShiftRows(): 数バイト単位で回転処理. 非線形の転置処理に相当. 4x4の行方向に対して行う.
  - MixColumns(): 4x4の列方向に対して, 行列を作用させる処理.
  - AddRoundKey(): 4x4行列の要素毎に共通鍵との排他的論理和を計算
- NISTにおける公開文書
  - http://csrc.nist.gov/CryptoToolkit/aes/

AES (2)

- Encryption algorithm
  - SubBytes(): bit transfer by byte unit, calculate inverse operator for polyinomial having x^8 as the highest order, corresponds to S-Box transfer
  - ShiftRows(): rotation at several byte unit. Non-linear transfer operated to 4x4 raw
  - MixColumns(): matrix applied to 4x4 column
  - AddRoundKey(): XOR operation to element of 4x4 matrix with common key
- Open documents at NIST
  - http://csrc.nist.gov/CryptoToolkit/aes/

Camellia (1)

- NTTと三菱電機が共同開発したブロック暗号 (2000)
  - 鍵長128ビット, 192ビット, 256ビット, ブロック長128ビット, ラウンド数は18段, 24段
  - Feistel構造
  - AESと同等の安全性
  - 基本特許は無償化(2001)
- IETFで標準化
  - Algorithm: RFC3713, RFC5528
  - S/MIME: RFC3657
  - XML Encryption: RFC4051
  - SSL/TLS: RFC4132, RFC5932
  - ...

Camellia (1)

- Block cipher developed by NTT and Mitsubishi electric (2000)
  - Key length 128, 192, 256 bit, block length 128 bit, round numbers 18, 24 steps
  - Feistel structure
  - Same level safety as AES
  - Basic patent is free (2001)
- IETF standardization
  - Algorithm: RFC3713, RFC5528
  - S/MIME: RFC3657
  - XML Encryption: RFC4051
  - SSL/TLS: RFC4132, RFC5932
  - ...

Camellia (2)

- S/MIME (Secure/Multipurpose Internet Mail Extensions)
  - MIMEでカプセル化した電子メールの公開鍵方式による暗号化とデジタル署名に関する標準規格
  - 電子メールソフトのために暗号技術を使ったセキュリティ機能(認証, 通信文の完全性(改竄防止), 発信元の否認防止(デジタル署名使用), プライバシーとデータの機密保護(暗号化使用))を提供
  - MIMEタイプ: application/pkcs7-mime(smime-type “enveloped-data”) を用いてデータが暗号化されたデジタル封書を実現
  - 通信文全体は暗号化され, 続いてapplication/pkcs7-mimeのMIMEエンティティに挿入されるCMSの書式に格納される

Camellia (2)

- S/MIME (Secure/Multipurpose Internet Mail Extensions)
  - Standard related to encryption and digital signature by common key algorithm for e-mail capusled by MIME
  - Provides security (certification, falsification protection), using encryption for e-mail, prevension of denial using digital signature, privacy and security
  - MIME type: application/pkcs7-mime(smime-type “enveloped-data”)
  - Message is encrypted, stored in MIME entity of application/pkcs7-mime

Camellia (3)

- SSL (Secure Sockets Layer)
  - セキュリティーを要求される通信のためのプロトコル
  - Transport Layer Securityとも呼ばれる
  - 共通鍵暗号に基づく暗号化を提供 (×:未対応, ○:選択, ◎:必須) またCamellia, SEEDを含む

アルゴリズム	SSL2.0	SSL3.0	TLS1.0	TLS1.1	TLS1.2
暗号化なし	×	○	○	○	○
RC2	○	○	○	○	×
RC4	○	○	○	○	○
IDEA	○	○	○	○	×
DES	○	○	○	○	×
トリプルDES	○	○	◎	◎	○
AES	×	×	△	○	◎

Camellia (3)

- SSL (Secure Sockets Layer)
  - Communication protocol required security
  - Called Transport Layer Security
  - Provides encryption based on common key system (×:no, ○:option, ◎:mandatory) includes Camellia and SEED

アルゴリズム	SSL2.0	SSL3.0	TLS1.0	TLS1.1	TLS1.2
暗号化なし	×	○	○	○	○
RC2	○	○	○	○	×
RC4	○	○	○	○	○
IDEA	○	○	○	○	×
DES	○	○	○	○	×
トリプルDES	○	○	◎	◎	○
AES	×	×	△	○	◎

WPA

- Wi-Fi Protected Access (WPA, WPA2)
  - Wi-Fi Alliance が策定したセキュリティプロトコル
  - Wired Equivalent Privacy (WEP) の脆弱性対策
- WPA
  - RC4ストリーム暗号, 鍵長128ビット, 初期化ベクトル48ビット
- WPA2
  - AES暗号ベースのアルゴリズム CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

WPA

- Wi-Fi Protected Access (WPA, WPA2)
  - Security protocol provided by Wi-Fi Alliance
  - Remedy for weakness of Wired Equivalent Privacy (WEP)
- WPA
  - RC4 stream encryption, key length 128 bit, initial vector 48 bit
- WPA2
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) algorithm based on AES

IPsec (1)

- IPSec (Security Architecture for Internet Protocol)
  - 暗号技術を用いてIPパケット単位でデータの改竄防止や秘匿機能を提供するプロトコル
  - 暗号化をサポートしていないトランスポート層やアプリケーションを用いても，通信路の途中で通信内容を覗き見られたり改竄されることを防止できる
- 構成
  - AH (Authentication Header) による完全性，認証機構
  - ESP (Encapsulated Security Payload) によるデータ暗号化等のセキュリティプロトコル
  - IKE (Internet Key Exchange protocol) などによる鍵交換

IPsec (1)

- IPSec (Security Architecture for Internet Protocol)
  - Protocol provides preventing falsification and security at IP packet unit using encryption technology
  - Even at transport layer and application which do not support encryption can have encryption function
- structure
  - AH (Authentication Header) provides authentification
  - ESP (Encapsulated Security Payload) provides security protocol for data encryption
  - IKE (Internet Key Exchange protocol) gives key

IPsec (2)

- IPsecが使えるシステム
  - Windows
    - 2000/XP/Vista IPv4, IPv6
  - Mac OS X
    - L2TP/Ipsec: KAME
  - BSD
    - FreeBSD, NetBSD: KAME
  - Linux
    - IPv4, IPv6 IKE: racoon

IPsec (2)

- System where IPsec can be used
  - Windows
    - 2000/XP/Vista IPv4, IPv6
  - Mac OS X
    - L2TP/Ipsec: KAME
  - BSD
    - FreeBSD, NetBSD: KAME
  - Linux
    - IPv4, IPv6 IKE: racoon