共通鍵暗号と
そのプログラムの利用

Common-Key Cryptographic and usage of the program

渡邊研究室
００J125　増田 真也

1. はじめに

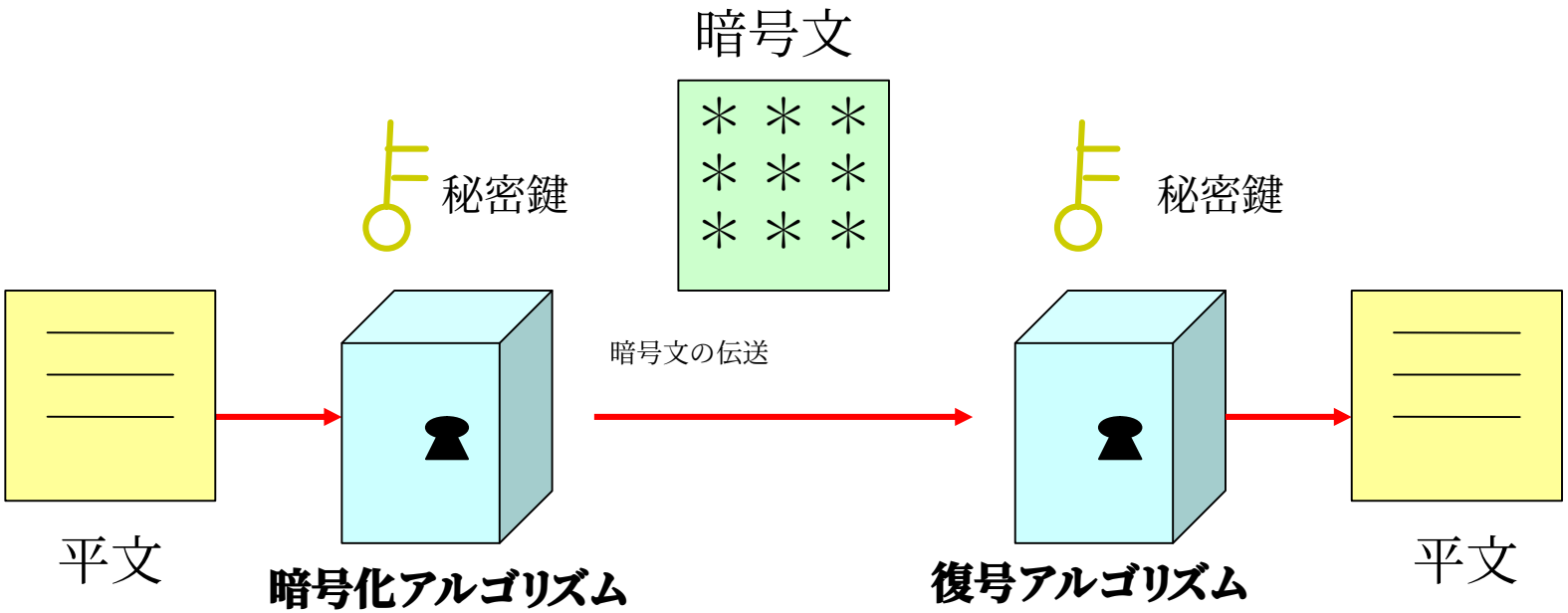
- 暗号化はネットワークの安全性において、コンピュータ処理の最も重要な手段
- 暗号の分類
  - 共通鍵暗号
  - 公開鍵暗号

1. はじめに

- 暗号化
  - 暗号化の仕組みは一般的に3つの軸で分類される
    - 平文を暗号文に変換する際に用いる演算のタイプ
      - 暗号化アルゴリズム ：換字と転置の2つの一般原則に基づく
    - 使用される鍵の数
      - **送信者と受信者が同じ鍵を使う → 共通鍵暗号**
      - 送信者と受信者が異なる鍵を使う → 公開鍵暗号
    - 平文を処理する方法
      - ブロック暗号
      - ストリーム暗号

2. 共通鍵暗号

- 共通鍵暗号のモデル



共通鍵暗号の概念図

3. 既存アルゴリズムの特徴

- DES
  - 1977年にIBMが開発
  - 64bit毎に処理するブロック暗号で、鍵長は56bit
    → 現在では安全とは言えない
- 3DES
  - DESの暗号化/復号処理を3回実行
  - DES用高速LSIの利用とDES実績がメリット
  - 処理が重い

3. 既存アルゴリズムの特徴

- MISTY
  - 1995年に三菱電機が開発
  - 64bit毎に処理するブロック暗号で、鍵長は128bit
    → DESよりも十分な安全性
- AES
  - DESに代わる時期標準規格の次世代共通鍵ブロック暗号
  - ブロック長は128bitで、鍵長は128,192,256bit
- Camellia
  - 2000年にNTTと三菱電機が共同開発
  - 128bit毎に処理するブロック暗号で、鍵長は128,192,256bit

4. プログラムの利用

- OpenSSL
  - SSLとTLSを実装した無償のライブラリ
  - DES、3DES、AESを始めとした多数の暗号アルゴリズムを実装
  - 利用形態
    - **プログラムから暗号化の処理を行う関数を呼び出す**
    - 実行ファイルを使用して暗号化の処理を行う

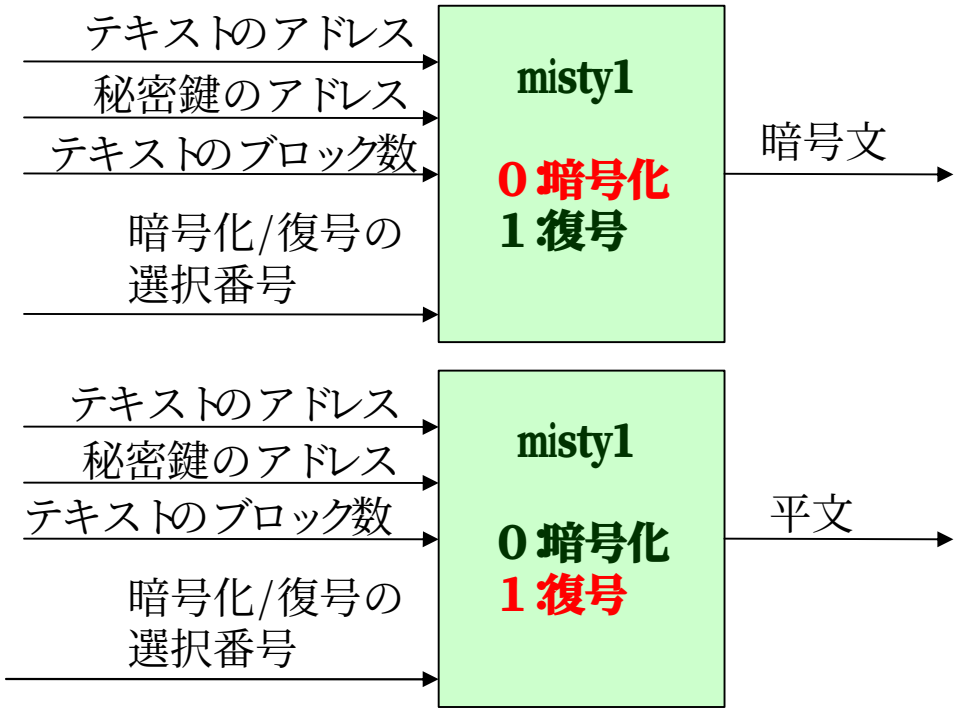
4. プログラムの利用

- MISTY 1のサンプルコードの応用
  - 題材
    - MISTYを開発した三菱電機の 松井 充 氏が作成した MISTY 1のサンプルコード

      http://www.security.melco.co.jp/Japanese/MISTY/misty_j.pdf

4. プログラムの利用

- 暗号化/復号の本体 misty 1の入出力関係



misty1の入出力関係

4. プログラムの利用

- 任意文字列を入力
  - サンプル :固定データ（16byte）のテキスト

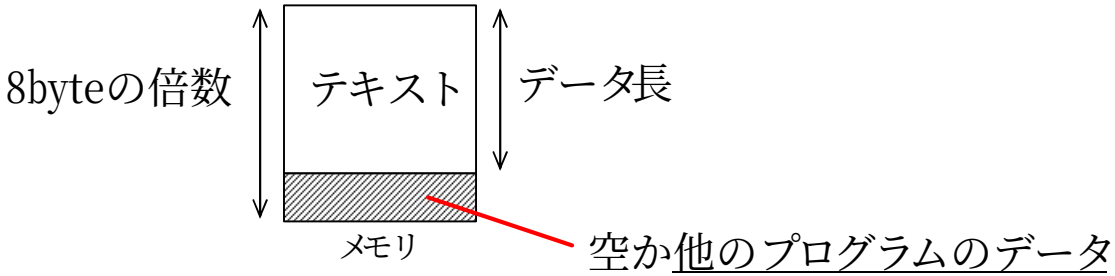
    → 任意文字列を入力して処理するように変更
  - サンプル :常に2ブロック

    → テキストのブロック数を算出する必要がある
    - 例）18文字の半角英数字を入力

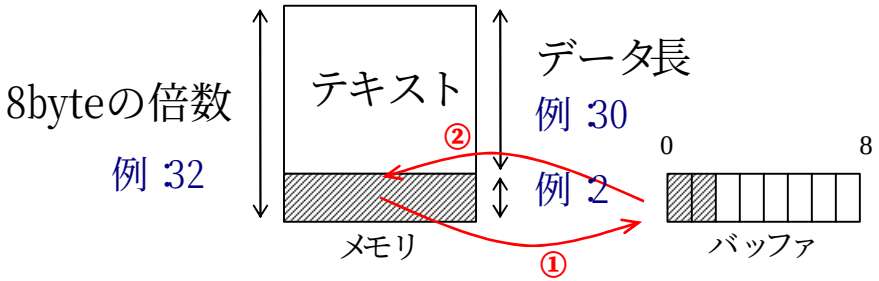
      → 要するブロック数は 3ブロック

4. プログラムの利用

- ブロック内の余りの考慮



ブロック内の余りの問題

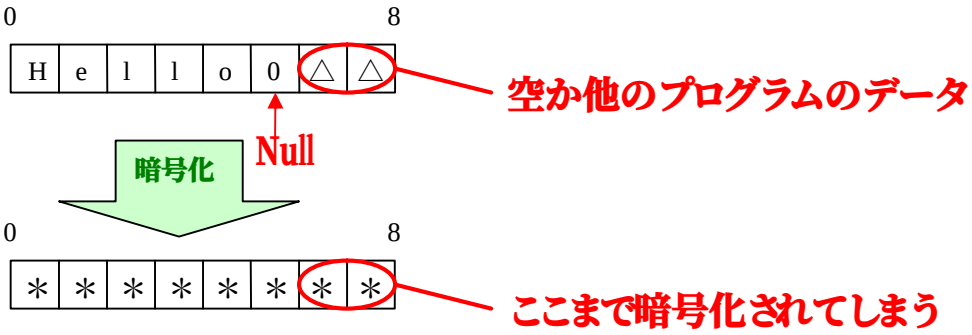


① 暗号化の前にバッファへ退避
② 暗号化して暗号データを出力後，退避したデータを元に戻す

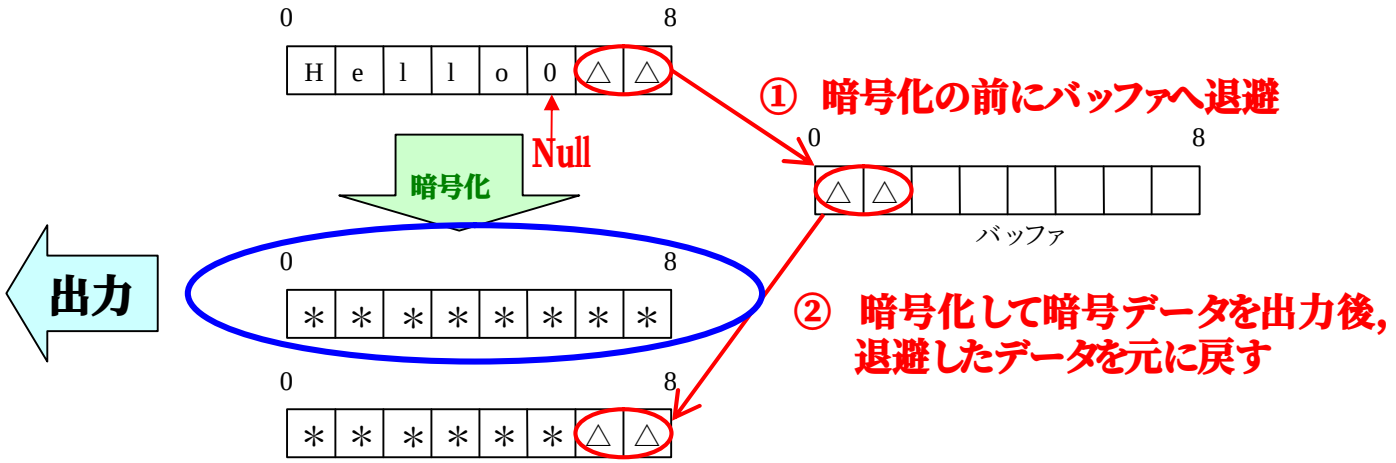
バッファへ退避することによる解決

4. プログラムの利用

- ブロック内の余りの考慮 ： 具体例



ブロック内の余りの問題の例



バッファへ退避することによる解決の例

5. 今後の課題

- OpenSSLでの暗号ライブラリの利用を調査
  - MISTY 1プログラムと差し替え可能な入出力関係であるか

    → 一般的な暗号ライブラリの入出力関係に合わせる必要がある
- パケットの暗号化を考慮したプログラム

  → 実際にパケットの暗号化・復号を試みる

おわり

参考文献

- 情報セキュリティ技術

  http://www.security.melco.co.jp/SecWWW/

- 暗号とネットワークセキュリティ　理論と実際」

  著：W・スターリンス　出版：㈱ピアソン・エデュケーション