- INSec#4 情報の防御
  - 暗号
    - いまだ解読されていない歴史的な10種の暗号 → http://gigazine.net/news/20110202_uncracked_codes/
    - 暗号とは？
      - E：暗号化アルゴリズム、D：復号アルゴリズム、K、K'：鍵
      - c = E (K, m) ／／メッセージmを暗号化し暗号文cを得る（暗号化）
      - m = D (K' , c) ／／暗号文cを復号しメッセージmを得る（復号）
    - 公開鍵暗号
      - →RSA暗号
        - 1976：W.Diffie, M.E.Hellman により概念の提案
        - 1978：R.Rivest, A.Shamir, L.Adleman により具体的方式の提案
      - 暗号化鍵と復号鍵が異なり、暗号化鍵から復号鍵を求めることが困難
      - 原理
        - 安全性の要件
          - 公開鍵より秘密鍵を求めることが困難
          - 逆に、秘密鍵より対応する公開鍵を生成することは容易
        - 安全性の証明
          - 「問題を解くことが困難ならば安全性が満たされる」
        - 安全性に関する問題
          - 素因数分解問題：
            与えられた合成数ｎより、ｎを割り切る素数ｐを求める
          - 離散対数問題：
            与えられた素数ｐとｙ、ｇより、ｙ＝ｇ^X mod ｐを満たすXを求める
        - アルゴリズム
          - 鍵生成アルゴリズム：
            乱数を用いて公開鍵と秘密鍵のペアを生成
          - 暗号化アルゴリズム：
            公開鍵とメッセージを入力し暗号化を行い、メッセージに対する暗号文を生成
          - 復号アルゴリズム：
            秘密鍵と暗号文を入力し復号を行い、暗号文に対するメッセージを生成
        - 公開鍵と秘密鍵は複数回利用
          - 暗号化回数に限界を持つ方式も存在
      - 実現できる機能
        - メッセージの秘匿性：
          暗号文より元のメッセージを求めることが困難…公開鍵を与えられても
        - 親展機能：
          秘密鍵を持つ特定の者のみメッセージを得ることが可能
        - 暗号化可能なメッセージの長さに制限
          - ハイブリッド法：
            1.メッセージを共通鍵暗号で暗号化
            2.共通鍵暗号の鍵データを公開鍵暗号で暗号化
            →送付・共有：鍵配送
      - 変遷
        - RSA暗号：メッセージに対し暗号文が1つ →
          RSA-OAEP：1つのメッセージに対し複数の暗号文、選択暗号文攻撃に対し安全
          - 選択暗号文攻撃(Chosen Ciphertext Attack)：
            解読者が指定する暗号文とそれに対応する平文の情報を手がかりとする暗号解読。
        - EIGamal暗号：1つのメッセージに対し複数の暗号文
        - Diffie-Hellman鍵交換
          - 離散隊数問題の困難性
          - 秘密鍵共有の代表的な方式
    - 共通鍵暗号
      - 暗号化に用いる鍵と復号に用いる鍵が共通＝秘密鍵暗号
      - ブロック暗号
        - 固定された長さのデータ(ブロック)の暗号化・復号を行う
        - ブロック長：64,128,192,256
        - DES(Data Encryption Standard)：64bitブロック-56bit鍵
        - MISTY：64bitブロック-128bit鍵
        - AES(Advanced Excryption Standard)：128bitブロック-128/192/256bit鍵
      - ストリーム暗号
        - 平文を1ビット単位で暗号化・復号を行う
        - 同期式、非同期式
    - 要素
      - ハッシュ関数
        - 任意長のデータを固定長のデータに(ハッシュ値)に圧縮
          - H：ハッシュ関数
            一方向性：与えられたｙに対して、ｙ=H(ｘ)を満たすｘを求めることが困難
            耐衝突性：H(a)＝H(b)を満たす互いに異なるａ、ｂを求めることが困難
        - 公開鍵暗号や電子署名の構成要素
        - MAC(Message Authentication Code：メッセージ認証符号)の構成要素
          - HMAC(Hash-based MAC)
        - パスワード管理 → パスワードのハッシュ値管理
        - 構成：「圧縮関数」を多段に繰り返す
          - Ron RiverのMD4
        - 代表的な専用ハッシュ関数：SHA1, MD5, RIPEND-160
      - 暗号用乱数
        - 要件：部分系列より他の部分系列を予測することが困難
          - 性質：
            統計的乱数性：出力乱数系列が一様分布と統計的に近い
            長周期性：出力乱数系列の周期が短くない
          - 線型複雑度：→大きいこと！
            線型フィードバックレジスタの最小サイズ
        - 疑似乱数
          - 疑似乱数生成器
          - 一方向性関数
      - 鍵管理
        - 鍵の更新！
        - 一時鍵、セッション鍵、作業鍵：メッセージの送受信時でのみ利用される共有鍵
        - 保管方法
          - 耐タンパ装置内で鍵生成
            - 耐タンパ性(tamper resistant)
              ソフトウェアやハードウェアが備える内部構造や記憶しているデータなどの解析の困難さ
          - キーリカバリシステム
            - 信頼できる第三者機関に秘密鍵のバックアップ
          - 秘密分散技術
      - ゼロ知識証明
        - 本人だけが知っている秘密情報を使った認証で、秘密情報自体を送受信することなく秘密情報を知っていることを証明する方法
    - その他の暗号方式
      - MAC(Message Authentication Code：メッセージ認証符号)
      - 量子暗号
      - 秘密分散
    - 暗号解読と強度評価
      - 全数探索型攻撃法
        - 全ての秘密鍵候補を試す
        - テーブル参照法
        - タイムメモリートレードオフ法
      - ショートカット法
        - 差分攻撃法
          - 高段差分攻撃法
        - 補間攻撃法
        - 線型攻撃法
        - 中間一致攻撃法
      - サイドチャネル法
        - タイミング攻撃法
        - 故障利用攻撃法
      - 暗号技術評価プロジェクト → http://www.cryptrec.go.jp/index.html
    - IDベース暗号
      - ID(メールアドレス等)そのものが暗号化で用いる公開鍵
      - 要素
        - セットアップアルゴリズム
        - 鍵抽出アルゴリズム
        - 暗号化アルゴリズム
        - 復号アルゴリズム
    - サルにもわかるRSA暗号 → http://www.maitou.gr.jp/rsa/rsa01.php