# CRYPTRECの活動

東京理科大学
金子敏信

# CRYPTRECにおける評価

- 電子政府用暗号技術のリストアップ
- 専門的・客観的見地から評価・調査
- 利用可能技術の特徴
  - 実装性、安全性等
- 一つの技術に絞ることを目的とはしない

# 一つにしぼらない

- 暗号技術の用途は広範囲
  - 応用システム側から種々の要求
  - ブロック長、HW
- 安全性
  - 用途によっては複数暗号使用

# 公募項目

- 公開鍵暗号
- 共通鍵ブロック暗号
  - ブロック長64、128
- ストリーム暗号
- ハッシュ関数
- 乱数生成技術

# 評価の観点

- 第３者実装が可能な情報公開
  - 設計指針から仕様まで
- 安全性
  - 代表的な攻撃に対する耐性
  - その暗号固有の攻撃に対する耐性
- 実装性
  - 速度、
  - 実装規模

# 評価プロセス

- 公募　４８件　　(2000. 7. 14)
- スクリーニング評価 (2000. 8ー9)
  - 詳細評価に対する適否
- 詳細評価　　(2000. 10―2001. 3)