2010 年度 情報処理システム製作
（4 名以上，10 名まで）

暗号入門

担当 宮道

創作教室：サルではわからない現代暗号

目標：

（１）秘密鍵暗号、公開鍵暗号、ディジタル署名、認証、一方向性関数、落し戸付き一方向性関数、ナップザック問題、離散対数問題、ＲＳＡ、楕円曲線暗号、超楕円曲線暗号、代数曲線暗号、DH鍵交換方式、IDベース暗号 などが何なのかを理解する.
（２）有限体、捩じれ点，デバイザー、ペアリング等を理解する。
（３）Ｊａｖａの勉強をし，簡単な暗号作成プログラムをつくる.
（４）実用的な（？）暗号作成プログラムを作成する.
（５）新しい暗号方式を発明し、世界的に有名になる.
（または、公表しないで会社を設立し大金持ちになる. ）
（または、世の中にはすごい人がいることを実感する. ）

暗号はクイズです。楽しむことが大事。
システム製作なのか、単なる勉強会なのか、それは君次第。

○株式会社秀和システム
『Ｊａｖａで学ぶ
暗号プログラミング』
○共立出版株式会社
『暗号理論の基礎』
○ シュプリンガーフェアラーク
『数論アルゴリズムと
楕円暗号理論入門』