科目区分：自然科学

授業科目名	数理科学（暗号の数理）					学期	曜日	校時
英　語　名	Mathematical Science (Cryptography)							
担　当 教　官　名	末吉　豊	単位数	2単位	必修 選択	選択	後期	水曜日	II校時

授　業　の　ね　ら　い　・　内　容　・　方　法

約 25 年前，公開鍵暗号の出現により，暗号の概念は一変した．コンピュータの発達，インターネットの急速な普及に伴い，情報の安全な通信が求められているが，現代暗号は，情報社会を支える重要な技術となっている．この講義では，古典暗号から現代暗号に至るまで，暗号の仕組みをわかりやすく解説する．

テ　キ　ス　ト　、　教　材　等

プリントを配布する．参考図書は講義の中で紹介する．

対　象　学　生	成　績　評　価　の　方　法	教　官　研　究　室
全学部	平常点(演習・小テスト・レポート) 50% 中間・期末試験 50%	

授　　業　　計　　画

古来，暗号は軍事・外交面で情報の秘匿のために用いられてきた．しかし，約 25 年前，公開鍵暗号とよばれる画期的な暗号方式が発明された．この暗号では暗号化鍵を公開するが，秘密の復号化鍵は容易にわからない．公開鍵暗号に対して，古来より知られている暗号方式は共通鍵暗号（または秘密鍵暗号）とよばれるが，公開鍵暗号の発明と時を同じくして，共通鍵暗号も情報化社会の要請に応えるべく進化した．公開鍵暗号と進化した共通鍵暗号を用いることにより，インターネットで情報を安全に送ったり，通信相手の身元を確認したりすることが可能になり，電子商取引，電子マネー，電子投票，電子政府などを実現できる．

講義では，シーザー暗号などの古典暗号より始めて，高度情報化社会の重要な基盤となっている現代暗号の数理的仕組みをわかりやすく紹介する．最先端の数学が最先端の技術に貢献していることを理解して頂けると嬉しい．予備知識としては，高校の数学Ⅰ，II，A程度で十分である．授業は，講義と演習を２：１の割合で構成する．

（授業計画）

１．現代暗号と情報社会（秘密通信とディジタル署名）
２．古典暗号
３．古典暗号の解読
４．進化した共通鍵暗号
５．ユークリッドの互除法
６．合同式
７．RSA 暗号，RSA 署名
８．e-コマースのセキュリティ（SSL と SET の仕組み)
９．中間試験
１０．有限体
１１．離散対数問題
１２．Elgamal 暗号と Diffie-Hellman 鍵配送
１３．楕円曲線
１４．楕円曲線暗号
１５．期末試験

（受講者への要望）

論理的な思考力，判断力，表現力を身につけるのがねらいであるので，授業に積極的に参加すること．また，演習問題に真剣に取り組むこと．