暗号理論 ～暮らしを支える数学～

竹内裕隆
慶應義塾大学理工学部 1 年

2014 年 10 月 18 日

1　始めに

メールの送受信，電話，ウェブ検索，SNS の使用，ネットショッピング.....．私たちはこれらの事をインターネットを介して行っています．しかし，インターネットの通信網は，この回線は誰々専用，といった感じではなく，基本的には共用の物です．つまり，例えば自分が誰かに送ったメールを他の誰かが盗み見する，という事が容易に起こっても不思議ではありません．安全にインターネットを使うためには，送りたい情報を第三者にはわからない様に加工して送る必要があります．大ざっぱに言ってしまえば，この情報を加工するというのが暗号化するという事です．私たちはこの暗号化に関する理論によって，ネット社会を日々安全に暮らしています．そして，暗号理論は他の情報理論同様，数学の理論を土台として成り立っています．

2　内容

今回は主に代数学と初等整数論についてさっくりと説明した後に，公開鍵暗号を 2，3 個見ていきます．公開鍵暗号の安全性は計算量理論によるものですが，それを知らなくても，暗号の仕組みや特徴は理解できるので，あまり触れません．前提知識としては整数の足し算，行列の掛け算，置換の積について知っていれば十分です．厳密な議論はあまりせず，数学がどんな風に役立っているかを見ていこうと思っているので，気軽に聞いてください．

参考文献

[1] 一松信，暗号の数理　〈改訂新版〉　作り方と解読の数理　講談社（2005）

[2] 宮地充子，代数学から学ぶ暗号理論：整数論の基礎から楕円曲線暗号の実装まで　日本評論社 (2012)

[3] 津村博文，代数学，テキスト理系の数学　数学書房（2013）

[4] James, J. T.，初等整数論 9 章　森北出版（2008)