レポート課題3

- 締め切り:７月８日
- 書式は自由、メールにて提出してください。
  宛先:
  webseminar@satolab.itc.u-tokyo.ac.jp
- Subject(件名)にWebseminar Report 3と書いてください。

問題

- 暗号文を作成し、提出せよ。
- また、提出された暗号文の復号の方法を説明せよ。ECCSのiMac端末で復号することを前提とし、使用するコマンドまで詳細に記述すること。
- 平文（元の文）に含めるべき情報は、学籍番号と氏名（ローマ字も可）とする。
- 我々が保持する秘密鍵(RSA)に対応する公開鍵を下記で公開しているので使用して構わない。
  `http://www-sato.cc.u-tokyo.ac.jp/PKI-project/Komaba/webseminar.pub.txt`

注意

- 暗号文は大抵バイナリファイルなので添付ファイルとして提出すると良い。
- メールが配送される経路は盗聴される危険性があるものとし、盗聴した第三者が暗号文を解読できないように工夫すること。（例えば、共通鍵暗号を用いて暗号化して鍵をメール本文に書く、は不可）