情報セキュリティ（佐竹 賢治）後期　2007/01/24

問題用紙　表と裏の２ページ

１．文章の穴埋め（記号選択式で名詞。解答群（１８個くらい）から選択）出題数１２問。
文章のニュアンスは正確ではないけど、大体こんな感じのものが出題された。
「」の単語は解答に当たる部分です。or があるとこはわからんかったw調べてw
基本的にノートに書いた定義の文章がそのまま書いてあります。

- b = q･a + r (0 < = r < a)の r を「剰余」という。r が 0 のとき b は a に「整除」されるという。
- (a, b) = 1 のとき a と b は「互いに素」という。※a と b の最大公約数が１って意味。
- 「体」の定義は①F は「加法群」である②F* = F - ｛ 0 ｝は「可換群」である
- 乗法群 G においてすべての元 x が～～～～～～の場合、群 G を「巡回群」という。またこの a を「原始元」という。
- DES 暗号の s-box は「線形置換 or 非線形置換」によって暗号強度を高めている。
- バーナム暗号は「計算量的 or 情報量的」に安全である。
- ～～～～は「ユークリッド互除法（たぶん・・・）」と呼ばれる

２．(1)**オイラー関数の**φ(18)**を求めよ。**Answer　**６**
(2)5･x ≡ 1 mod 18 **を満たす** x **を求めよ**　　Answer 11
(3)7 **の９８乗を１８で割った余りを求めよ（数式で表現してある）** Answer 13

３．(1)**ＲＳＡについて説明せよ（語句の説明問題）**
(2)e = 7,p = 5, q = 11 **のとき、秘密鍵** d **を求めよ。**
(3)**平文** M = **整数（具体的な数字忘れたw）のとき、暗号化されたＣ（暗号化した結果のこと）を求めよ**