2014 年度 春・(秋)学期定期試験						問題枚数	1/1
科目名		出題者氏名	受験クラス	学生証番号		氏名	
暗号理論		山本宙	JT, その他				
持込	不可	◇可の場合は，記入	開講曜日・時限	現在使用している授業教室	4101 コンピュータ室	採点	
	(可)	関数電卓	水曜 3 限				

注意事項

答案は解答用紙に書け．答案用紙の裏を使用する場合は表の最後に「裏に続く」と記入せよ．諸定義は以下の通りとする．

mod ：a を n で割った余りを $a \pmod n$ と表す
オイラー関数 ：オイラー関数を $\phi(n)$ と表す
自然数 ：0 以上の整数
素数 ：2 以上の整数で 1 と自分自身以外の約数をもたないもの
互いに素 ：整数 a, b の最大公約数が 1 のとき，a, b は互いに素
約数 ：整数 a を正整数 b で割った余りが 0 のとき b は a の約数

問 1 (各 5 点，計 30 点)

以下の問に答えよ．

1-a) $5^2 \pmod{32}$ を求めよ　**1-b)** $5^5 \pmod{32}$ を求めよ　**1-c)** $5^{46} \pmod{32}$ を求めよ
1-d) Z_{15}^* の要素を全て書け　**1-e)** $\phi(15)$ の値を書け
1-f) 整数 n と，n と互いに素な整数 a に対し，$a^{\phi(n)} \pmod n$ の値について，以下**ア．イ．**のどちらが正しいか，記号で答えよ．**ア．**必ず 1 になる，**イ．**1 になることも，それ以外の値になることもある．

問 2 (各 2 点，計 8 点)

以下の問いについて，内容が正しいものに○，間違っているものに×を解答欄に書け．

2-a) 暗号化は，暗号化鍵というパラメータに依存する変換である．
2-b) 現代の暗号では暗号化アルゴリズムを知れば鍵を知らなくても平文を得られる
2-c) 公開鍵暗号系では復号化鍵を公開しても情報の秘密が保てる．
2-d) 対称鍵暗号系では暗号化鍵と復号化鍵が同一でなければならない．

問 3 (各 3 点，計 12 点)

暗号アルゴリズムはいくつかの計算が実用的な時間では不可能であるという前提で構成されている．以下のうち，この意味で実用的に計算可能とされているものには○，不可能とされているものには×を答案用紙に書け．ここで，p, q は大きな素数とする．

3-a) $pq = n$ のとき，p と q から n を求める
3-b) $pq = n$ のとき，p, q から $\phi(n)$ を求める
3-c) $Y \equiv a^X \pmod p$ のとき，Y, a, p から X を求める
3-d) $(p-1)(q-1)$ と e が互いに素かどうかを判定する

問 4 (4-a 5 点，4-b 5 点，4-c 15 点，計 25 点)

RSA 暗号において $p = 5, q = 11$ とする．すなわち $n = 55$ となる．

4-a) e の値として 18 が暗号化鍵に使えない理由を述べよ．
4-b) 以下 $e = 13$ とする．平文 $M = 40$ を暗号化した暗号文を求めよ．
4-c) 暗号化鍵 e に対応する複合化鍵 d を求めよ．ただし，u, v に対するユークリッド互除法のアルゴリズムは以下のアルゴリズム 1.1 である．答案用紙には各ステップでの (u_1, u_2) の値と（u_3 は不要)，最終的な d の値を書け．

アルゴリズム 1.1

S1) $(u_1, u_2, u_3) = (1, u, 0)$, $(v_1, v_2, v_3) = (0, v, 1)$
S2) $v_2 \neq 0$ である限り，以下を繰り返す
　$w = \lfloor u_2/v_2 \rfloor$　　($\lfloor\ \rfloor$ は整数部分を示す)
　$(t_1, t_2, t_3) = (u_1, u_2, u_3) - (v_1, v_2, v_3)w$
　$(u_1, u_2, u_3) = (v_1, v_2, v_3)$
　$(v_1, v_2, v_3) = (t_1, t_2, t_3)$
アルゴリズムが停止したときの u_1, u_2, u_3 が出力で，$u_2 = gcd(u, v)$, $u_1 u + u_3 v = u_2$ を満たす．

問 5 (10 点)

鍵階層について，階層数 2 で対称暗号と非対称暗号が使われるとき，多くの場合どちらがデータ暗号に使われるか，理由とともに述べよ．

問 6 (各 5 点，計 15 点)

DH 公開鍵暗号方式について，ノード i の秘密情報を X_i, 公開情報を Y_i とする．全ノードの秘密情報と公開情報には $Y_i \equiv a^{X_i} (\mathrm{mod}\ p)$ の関係がある．$p = 13$, $a = 7$ であるとき，以下の問いに答えよ．

6-a) 秘密情報 $X_A = 5$ であるノード A の公開情報 Y_A を求めよ．

6-b) 秘密情報 $X_B = 8$ であるノード B の公開情報 Y_B を求めよ．

6-c) 上記の場合，DH 公開鍵方式でノード A と B が秘密に共有するワーク鍵 WK_{AB} をノード A が求めるときの計算式と結果の数値を書け．