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	
認証技術		山本宙	JT, その他				
持込	不可 (可)	◇可の場合は，記入 関数電卓のみ	開講曜日・時限 火曜 2 限	現在使用している授業教室	4105 教室	採点	

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授業と同じものとする．

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
mod ：a を n で割った余りを $a \pmod n$ と表す
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
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
オイラー関数 ：オイラー関数を $\phi(n)$ と表す

問 1 (各 3 点，計 36 点)

以下の問に答えよ．

1-1) 0 以上 100 未満の整数で，mod 20 で 7 と合同なものを全て書け．
1-2) $a \equiv b \pmod n$ のとき，すべての x について $x + a \equiv x + b \pmod n$ が成立するかどうか答えよ．
1-3) $3^2 \pmod{10}$ を求めよ　　**1-4)** $3^8 \pmod{10}$ を求めよ
1-5) $3^{50} \pmod{10}$ を求めよ　　**1-6)** Z_6 の要素を全て書け
1-7) Z_6^* の要素を全て書け　　**1-8)** $\phi(6)$ の値を書け
1-9) $\phi(10)$ の値を書け
1-10) 整数 n と，n と互いに素な整数 a に対し，オイラーの定理によると a の何乗が mod n で 1 になるか書け
1-11) 整数 a に対し，$a^r \pmod n = 1$ を満たす最小な正整数 r をベキ数という．$(\mathrm{mod}\ 10)$ のときの 9 のベキ数を答えよ
1-12) ベキ数が $\phi(n)$ となる数 a を原始根という．$(\mathrm{mod}\ 10)$ のときの最小の原始根を求めよ

問 2 (各 2 点，計 6 点)

平文アルファベットを 2 文字分アルファベットの順番で後にずらした文字に置き換える暗号例を考える．以下の問いに答えよ．

2-1) 暗号文が pgvyqtm だったとする．平文を書け．
2-2) ずらした量の “2” は暗号の要素の用語で何にあたるか書け
2-3) この例は**ア**．公開鍵暗号系，**イ**．対称暗号系，のどちらであるか記号で書け

問 3 (各 4 点，計 16 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．

3-1) $pq = n$ のとき，n から p と q を求める
3-2) $Y \equiv a^X \pmod p$ のとき，X, a, p から Y を求める
3-3) $Y \equiv a^X \pmod p$ のとき，Y, a, p から X を求める
3-4) $(p-1)(q-1)$ と互いに素な e から $de \equiv 1 \pmod{(p-1)(q-1)}$ となる d を求める

問 4 (4-1 5 点，4-2 20 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．暗号化鍵を $e = 13$ とする場合，以下の問いに答えよ．

4-1) 平文 $M = 40$ を暗号化した暗号文を求めよ．
4-2) 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 (各 3 点，計 9 点)

以下の空欄を埋める適当な語句を答えよ．

- ハッシュ関数 $h(x)$ について，y が与えられて $y = h(x)$ である x を求めることが現実的に不可能である，という性質をもつハッシュ関数を[5-1]ハッシュ関数とよぶ
- ハッシュ関数 $h(x)$ について，異なる x_1, x_2 に対して $h(x_1) = h(x_2)$ となることが起きにくいハッシュ関数を[5-2]ハッシュ関数とよぶ
- 信頼できる機関がディジタル署名を施した公開鍵を公開鍵証明書といい，信頼できる機関を証明書発行機関という．証明書発行機関が別の証明書発行機関の公開鍵を署名し，証明書のチェインによって証明書発行機関の階層ができる．このような仕組みを[5-3]と呼ぶ．

問 6 (8 点)

次の表は RSA 署名のための公開鍵 (e, n) のリストである．いま，鈴木から佐藤あてに次のような署名文が届いた．この文を元にもどせ．ただし，$A = 0, B = 1, \ldots, Z = 25$,「スペース」$= 26$ とし，文字ごとに署名を掛けられているものとする．

署名文： 4,24

公開鍵：	(e, n)
佐藤：	(5,35)
鈴木：	(23,55)
田中：	(13,39)