2026年度

	暗号とインターネットセキュリティ	担当教員：福　光　正　幸	２単位

設　題

＜提出方法：インターネット提出＞

次の(1)～(4)の問いに答えなさい．ただし，S を解答者の学籍番号，s を解答者の学籍番号の下 5 桁からなる整数とする（例：学籍番号が 2370999 の場合，$S = 2370999, s = 70999$）．

(1) ユークリッドの互除法を用いて，次の整数の組の最大公約数を求めなさい．なお，この際に，わり算の表現について定義通り示すこと．

(A) $s, 5123$　　(B) $S, 15481$　　(C) $-S, 15481$

(2) 逆元に関して次の問題に解答しなさい．

(A) 法 m における値 a の逆元とは何か説明しなさい．

(B) 以下について，逆元が存在するかどうかを論じなさい．逆元が存在する場合は，逆元を求め，存在しないに場合は，その根拠を示しなさい．

① 法 108871 を基にしたときの s の逆元

② 素数 913247 を法としたときの $2^{913234} \bmod 913247 = 192861$ の逆元

(3) 学習用プリント p.9 にて紹介したバイナリ法に関して，次の問いに答えなさい．

(A) バイナリ法を用いることで，なぜ $a^x \bmod n$ の値を求めることができるか，その理由を解説しなさい．このとき，わかりやすさのため具体例を用いても良いが，具体例のみでなく，一般的に $a^x \bmod n$ の値を求められる理由の解説を要求する．

(B) バイナリ法を用いることで，次を求めなさい．このとき，計算過程も示すこと．ただし，③，④について，443が素数であることに注意すること．

① $7^{35} \bmod 37$　② $8^s \bmod 150$　③ $3^{27880} \bmod 443$　④ $3^{-27880} \bmod 443$

(4) 次の(A)～(E)の中から 1 つ選び，解答しなさい．

(A) ElGamal 暗号の鍵の作成，暗号化，復号の方法について調査し，まとめなさい．このとき，復号がうまくいく理由についても教科書の p.119 のようにして説明すること．

(B) ディジタル署名とはどのような技術であるかについて調査し，まとめなさい．また，併せて，その一例である Schnorr 署名について，鍵の作成，署名，検証の方法についても調査し，まとめなさい．

(C) 準同型暗号とはどのような技術であるかについて調査し，まとめなさい．なお，この技術を使った応用例について，考え論じなさい．

(D) ID ベース暗号とはどのような技術であるかについて調査し，まとめなさい．なお，この技術を使った応用例について，考え論じなさい．

(E) ブラインド署名とはどのような技術であるかについて調査し，まとめなさい．なお，この技術を使った応用例について，考え論じなさい．

レポート作成の際の注意点

- 解答について，Microsoft Word などの文書作成ソフトを用いて作成する方法の他，手書きの解答をスキャンし，PDF 化する方法も可能とする．
- 計算問題については，計算過程を示すこと．計算過程や根拠がない場合，大幅に減点する．
- 計算の根拠については教科書や学習用プリントで紹介された定義・定理・系を利用すること．
- 書籍や論文，Web 等を引用にした場合，その箇所が明確になるよう参考文献を記述すること．
- 引用物の定理・法則を利用したい場合，教科書や学習用プリントで紹介された定義・定理・系を用いて証明した上で用いること．
- 教科書に説明がない事実について，計算過程や参考文献がない場合は，大幅に減点する．

作成方法は「ワープロ」

ワープロ	用　紙　等：通信教育部標準フォーマット 作成した内容を Word もしくは PDF ファイルにして、提出期間中にポータルサイト「無限大キャンパス」から提出する。提出期間については、ポータルサイト「無限大キャンパス」にて確認すること。
文字数等	指定しない。横書き。