

|  |  | 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  |                  |           |     |
| <p>&lt;提出方法：インターネット提出&gt;</p> <p>次の(1)～(4)の問いに答えなさい。ただし、<math>S</math>を解答者の学籍番号、<math>s</math>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、<math>S = 2370999, s = 70999</math>）。</p>   |  |                  |           |     |
| <p>(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。</p> <p>(A) <math>s, 5123</math>                      (B) <math>S, 15481</math>                      (C) <math>-S, 15481</math></p>  |  |                  |           |     |
| <p>(2) 逆元に関して次の問題に解答しなさい。</p> <p>(A) 法 <math>m</math> における値 <math>a</math> の逆元とは何か説明しなさい。</p> <p>(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、存在しない場合は、その根拠を示しなさい。</p> <p>① 法 108871 を基にしたときの <math>s</math> の逆元</p> <p>② 素数 913247 を法としたときの <math>2^{913234} \bmod 913247 = 192861</math> の逆元</p>  |  |                  |           |     |
| <p>(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。</p> <p>(A) バイナリ法を用いることで、なぜ <math>a^x \bmod n</math> 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 <math>a^x \bmod n</math> の値を求められる理由の解説を要求する。</p> <p>(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が素数であることを注意すること。</p> <p>① <math>7^{35} \bmod 37</math>      ② <math>8^s \bmod 150</math>      ③ <math>3^{27880} \bmod 443</math>      ④ <math>3^{-27880} \bmod 443</math></p>              |  |                  |           |     |
| <p>(4) 次の(A)～(E)の中から1つ選び、解答しなさい。</p> <p>(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。</p> <p>(B) デ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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> |  |                  |           |     |
| <p><b>レポート作成の際の注意点</b></p> <ul style="list-style-type: none"> <li>● 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。</li> <li>● 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。</li> <li>● 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。</li> <li>● 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。</li> <li>● 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。</li> <li>● 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。</li> </ul>                     |  |                  |           |     |
| <p>作成方法は「ワープロ」</p>   |  |                  |           |     |
| ワープロ   | <p>用紙等：通信教育部標準フォーマット</p> <p>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。</p> |                  |           |     |
| 文字数等   | <p>指定しない。横書き。</p>  |                  |           |     |