駒澤大学 経営学部（担当： 西村和夫）

情報セキュリティ B 期末試験 **サンプル問題** （2009-09-16 版）

（持込みは，自筆ノート A4 判 1 枚だけ）

この用紙に解答を記入し，提出する． 自筆ノート（1 枚）もともに回収するので，右下に 学生番号，氏名 を記入しておくこと．

1. 次の文章のうち，正しいものは ○ を，誤っているものは × を解答欄に記入しなさい．[20 点] **解答欄**

(1) 虹彩による個人識別が可能であり，実際に使われている． (1) [ ]
(2) コナン・ドイルの“踊る人形”では，原字 t の頻度がもっとも高いことが解読の手がかりになった． (2) [ ]
(3) ビジュネル暗号は，綴（つづり）字換え字式暗号の一種である． (3) [ ]
(4) 通常の文章を単換え字式暗号によって暗号文にした場合，暗号文だけからでも解読は容易である． (4) [ ]
(5) 暗号に解読不可能なものはない．ただ，解読するのに莫大な時間がかかるものがあるだけである． (5) [ ]
(6) RSA 方式は，ハミルトン経路問題のむつかしさに基づく暗号方式である． (6) [ ]
(7) 現在の暗号技術を使っても，通信回線を使って不正のないポーカーをすることは，まだできない． (7) [ ]
(8) 日本語の文を平仮名だけで書いたとき，もっともよく現れる文字は“の”である． (8) [ ]
(9) JIS X 0208 にある文字（普通のワープロの文字）では，平仮名のほうがカタカナよりも 2 字多い． (9) [ ]
(10) AES（新データ暗号化規格）は，64 ビットのデータを 56 ビットの鍵で暗号化する方式である． (10) [ ]

2. 次の各文章の [ ] に入る適切なものを，それぞれの選択肢から選び，その記号 a～e を解答欄に記しなさい．[40 点]

(1) 日本語の文を平仮名だけで書いたとき，もっともよく現れる文字は [ ] である． **解答欄**
a. い e. う i. し n. た t. の (1) [ ]

(2) 暗号文を正当な受信者が通信文に戻すことを，[ ] という．
a. 解読 e. 組立て i. 盗聴 n. 復号 t. 復号化 (2) [ ]

(3) 通信文の発信者を保証することを，[ ] という．
a. 個人識別 e. 自己保全 i. 正当化 n. 認証 t. 発信者検証 (3) [ ]

(4) ヴァーナム (Vernam) 暗号は，[ ] 暗号の一種である．
a. 多表式 e. 単換え字式 i. 綴字換え字式 n. 転置式 t. 分置式 (4) [ ]

(5) 次のうち転置式暗号の一種であるのは，[ ] 暗号である．
a. 回転グリル e. シーザー i. ビジュネル n. ヴァーナム t. AES (5) [ ]

(6) 通信文 DOG と鍵 BAT から作った，ビジュネル暗号による暗号文は [ ] である．
a. EOZ e. ENW i. FOS n. FPA t. GPA (6) [ ]

(7) 通信文 CHANE を置換（2 1 4 5 3）（数値は暗号文における各文字の元の位置番号）によって転置した暗号文は [ ] である．
a. ANECH e. EANCH i. HCNEA n. HCEAN t. NEACH (7) [ ]

(8) 公開鍵暗号系で A から B に内容を秘匿する通信をするとき，受信者 B が使用する鍵は [ ] である．
a. A の公開鍵 e. A の秘密鍵 i. B の公開鍵 n. B の秘密鍵 t. 共通の秘密鍵 (8) [ ]

(9) 法が 7 のとき，5^3（5 の 3 乗）の値 v（$0 \leqq v < 7$）は [ ] である．
a. 2 e. 3 i. 4 n. 5 t. 6 (9) [ ]

(10) 法が 5 のとき，4 の（乗法の）逆元は [ ] である．
a. 0 e. 1 i. 2 n. 3 t. 4 (10) [ ]

3. 次の各問いに対する答えを，それぞれの選択肢 ア～エ から選び，その記号を**裏面**の解答欄に記しなさい．[20 点]

(1) セキュリティのガイドラインで，良いパスワードの例を出すことにした。鈴木さんの利用者 ID が，"1kr045se" のときに，良いパスワードはどれか。
a. c&wo3tk#g e. ikuzus n. kzs t. 1kr045se

(2) 公開鍵暗号方式に関する記述のうち，適切なものはどれか．
a. AES は，NIST が公募した公開鍵暗号方式である．
e. RSA は，素因数分解の計算の困難さを利用した公開鍵暗号方式である．
n. 公開鍵暗号方式に参加する利用者の数が増えると鍵の配送が煩雑になる．
t. 通信文の内容の秘匿に公開鍵暗号方式を使用する場合は，受信者の復号鍵を公開する．

（裏につづく）

駒澤大学 経営学部（担当： 西村和夫）

情報セキュリティ B 期末試験 **サンプル問題** （2009-09-16 版）

（持込みは，自筆ノート A4 判 1 枚だけ）

3. （つづき）

(3) ファイルにアクセス権が設定できる OS がある．このアクセス権の設定方法について，次の説明があった．

- アクセス権には，読取り，書込み，実行の 3 種類がある．
- この 3 種類のアクセス権は，それぞれに 1 ビットを使ってアクセスの許可・不許可が設定できる．ディレクトリには，合計 3 ビットの情報として設定する．
- この 3 ビットを 2 進数で表現し，000～111 で設定する．

この説明の後で，設定の試行を行った．次の試行結果から考えて，正しい記述はどれか．

〔試行結果〕

(a) 000 を設定したら，一切のアクセスができなくなってしまった．
(b) 011 を設定したら，書込みと実行はできたが，読込みができなかった．
(c) 111 を設定したら，すべてのアクセスができるようになった．

a. 010 を設定すると，読込みと書込みができる．
e. 100 を設定すると，読込みだけができる．
n. 101 を設定すると，実行だけができる．
t. 110 を設定すると，書込みだけができる．

(4) ある商店が，顧客からネットワークを通じて注文（通信文）を受信するとき，公開鍵暗号方式を利用して，顧客が誰であるかを確認したい．顧客，商店それぞれが利用する鍵の適切な組合せはどれか．（凡例 利用者：利用する鍵）

a. 顧客：顧客の秘密鍵， 商店：商店の公開鍵 （正しい選択肢はない！）
e. 顧客：顧客の秘密鍵， 商店：商店の秘密鍵
n. 顧客：商店の公開鍵， 商店：顧客の公開鍵
t. 顧客：商店の公開鍵， 商店：顧客の秘密鍵

(5) ディジタル署名を通信に利用する主な目的は二つある。一つは，メッセージの発信者を受信者が確認することである。もう一つの目的はどれか。

a. 署名が行われた後でメッセージに変更が加えられていないかどうかを，受信者が確認すること
e. 送信の途中でメッセージが不当に解読されていないことを，受信者が確認すること
n. 発信者の ID を受信者が確認すること
t. 秘密鍵を返信してよいかどうかを受信者が確認すること

解答欄 (1) [ ] (2) [ ] (3) [ ] (4) [ ] (5) [ ]

4. 次の各行為はどの法律・法令に違反するか，その名称（略称でよい）を，解答欄に記しなさい．[10 点]

(1) 不正に入手した他人の利用者名とパスワードを使って，プロバイダのメールサーバにアクセスし，他人の電子メールを閲覧した．ｰ **解答欄** (1) [ ] および [ ]

(2) インターネットのオークションに実在しない商品を出品し，落札者に現金を振り込ませてだまし取った．

解答欄 (2) [ ]

5. 次の内容を表す式を，解答欄に記しなさい．[8 点] **解答欄**

(1) 文字が n 種類であるときのシーザー式暗号（文字ずらし式暗号）の鍵の総数． (1) [式:]

(2) ブロックの大きさが n 文字であるときの転置式暗号の鍵の総数． (2) [式:]

6. 情報理論的に解読不可能な暗号を作成する具体的な方法を，下に記しなさい．ただし，鍵は具体的でなくてよい．[8 点]

このサンプル問題は暗号に偏っているが，実際には他の単元からももう少し出題する．

書かなかった場合は発表しない→ 成績発表のための暗証番号（1 けたの数字）→ □ 学生番号の末尾 2 桁＿＿＿＿