2009年7月8日

情報セキュリティ大学院大学
情報セキュリティ研究科（博士前期課程）情報セキュリティ専攻
2010年度特待生選抜試験問題

1次選考（筆記試験）

10:00～11:30

Ⅰ数学A
Ⅱ数学B
Ⅲ通信ネットワーク
Ⅳ情報システムA
Ⅴ情報システムB
Ⅵソフトウェア
Ⅶ暗号技術
Ⅷ経済
Ⅸ経営
Ⅹ法律

【注意事項】

1. 指示があるまで、この問題冊子を開いてはならない。
2. この問題冊子の本文は全部で20ページある。落丁、乱丁があれば申し出ること。
3. 上記Ⅰ～Ⅹの10項目から2項目を選択し、解答すること。10項目中どの2項目を選択してもよい。
4. 解答用紙は2枚配布される。選択した項目ごとに解答用紙を1枚使用すること。必要があれば裏面を使用してよい。
5. 解答用紙の指定欄に、選択した項目名、受験番号を必ず記入すること。解答用紙の回収前に、これらを記入したかを必ず確認すること。
6. 問題冊子、解答用紙、計算用紙は持ち帰ってはならない。

I 数学 A

$n = 16$ とし、$p = n^2 + 1 = 257$ とする。p は素数である。また、$a = 131$, $a_0 = 225$ とする。これらは

$$a_0 \equiv a^n \bmod p$$

を満足する。さらに、$b = 7$, $b_0 = 128$ とする。これらは

$$b_0 \equiv b^n \bmod p$$

を満足し、b は

$$b^{128} \not\equiv 1 \bmod p$$

を満足する。

以下の問いに答えよ。

(1) 合同式

$$c_i \equiv b_0^i \bmod p$$

を満足し、かつ $0 \leq c_i < p$ を満足する整数 c_i を $i = 0, 1, 2, 3$ に対して求めよ。

(2) 合同式

$$d_i \equiv a_0 b_0^{4i} \bmod p$$

を満足し、かつ $0 \leq d_i < p$ を満足する整数 d_i を $i = 1, 2, 3, 4$ に対して求めよ。

(3) 合同式

$$a_0 \equiv b_0^{x_0} \bmod p$$

を満足し、かつ $0 \leq x_0 < n$ を満足する整数 x_0 を求めよ。

(4) 合同式

$$b_1 \equiv b^{x_0} \bmod p$$

を満足し、かつ $0 \leq b_1 < p$ を満足する整数 b_1 を求めよ。

(5) 合同式

$$a \equiv b^x \bmod p$$

を満足し、かつ $0 \leq x < n^2$ を満足する整数 x を求めよ。

II 数学 B

Lを任意の言語とする。文字列xと文字列yがL**によって識別可能である**とは、ある文字列zがあって (xとzを連結した文字列である) xzか (yとzを連結した文字列である) yzのどちらか一方のみがLに属することをいう。文字列の集合XがL**によって対ごとに識別可能である**とは、Xに属するどの2つの異なる文字列もLによって識別可能であることをいう。Lによって対ごとに識別可能であるような集合Xの最大要素数を言語Lの**指数**と呼ぶ。

$\Sigma = \{a, b\}$をアルファベット集合とする言語

$$B = \{w \in \Sigma^* \mid w \text{は部分文字列として} baba \text{を含む}\}$$

について、以下の問いに答えよ。

(1) 文字列baと文字列babは言語Bによって識別可能であることを示せ。

(2) 言語Bの指数を求めよ。

Ⅲ通信ネットワーク

インターネットを利用して通信を行う場合、LAN の内部で使用するプライベート IP アドレスをグローバル IP アドレスに変換する必要がある。このアドレス変換機能は NAT（Network Address Translation）と呼ばれる。NAT について、下記の（1）から（3）に解答しなさい。なお、図を作成して解答に用いてもよい。

（1）NAT では IP アドレスのみでなく、アプリケーションサービスの種類やクライアントを識別するためのポート番号を一緒に変換することが多い。LAN 内部からインターネット上に公開されている Web サービスを利用する場合を例に、IP アドレスとポート番号が変換される様子を簡単に示せ。

（2）NAT はクライアント・サーバ型通信を想定した機能であるため、ピア・ツー・ピア P2P 型通信では NAT が支障となり通信できないことがある。NAT が支障となり通信できない、とは具体的にどのようなことを示すか。簡単に説明せよ。

（3）（2）で述べたことから、P2P 型通信では NAT の機能をかいくぐる、いわゆる“NAT 越え”の技術を適用している。“NAT 越え”の技術を 2 つあげそれぞれの概要を述べよ。

Ⅳ情報システムA

次の４項目すべてについて、各々5行程度で答えよ。

（1） 仮想マシンとは何か、またその利用目的について述べよ
（2） パイプライン処理の目的と、その実現機構について述べよ
（3） プロセス・スケジューリングとは何か、またその目的について述べよ
（4） フォールト・トレラント・システムとは何か、またその実現要素技術を一つ挙げよ

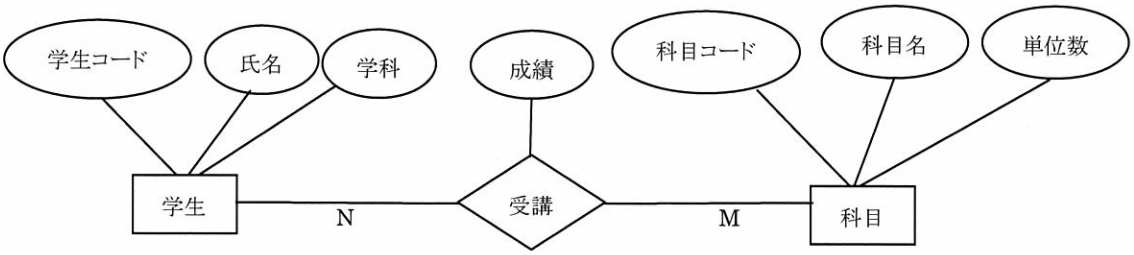
V情報システムB

情報システムのセキュリティ対策機能に関する次の項目について各々5 行程度で説明せよ。

（1） アクセス制御機能
（2） データ処理不正防止機能
（3） 情報漏えい防止機能

VIソフトウェア

次の図は、ある大学における成績管理システムの実体関連図である。



長方形は実体、ひし形は関連、楕円は実体および関連の持つ属性を表す。また、図では一人の学生は M 個の科目を受講し、一科目は N 人の学生により受講されていることを示している。

（問 1)　上記実体関連図をリレーショナルデータベース管理システムにおけるリレーショナルスキーマに変換し、変換後のリレーショナルスキーマを「リレーション名（属性名、・・・)」の形式で示せ。

（問 2)　各リレーションにおける主キーを示せ。

（問 3)　上記リレーションに対する問い合わせを実行する SQL 文を示せ。SQL 文は、
「select　属性名, ¨, 属性名　from リレーション名
　　where　条件文　　」
で表す。

(i)　学生「佐藤太郎」の科目名「代数」の成績は何か？
(ii) 科目名「電磁気学」の単位数はいくつか。

（問 4) 上記実体関連図に講師の情報を追加せよ。また、その時のリレーショナルスキーマを示せ。講師は、氏名と講師コードを持つ。一つの科目は複数の講師が担当する可能性がある。一人の講師は、二つ以上の科目を担当する可能性がある。

（問 5) このシステム運用開始後、他の（複数の）大学との間に単位互換制度が発足した。つまり、「他大学の学生も受け入れ、他大学での取得単位も当大学の単位として認める」制度である。この時、上記　成績管理システムをどのように変更し、また運用していけば良いか。

VII 暗号技術

p を奇素数とし，奇素数 q を $p-1$ の約数とする．$g \in (\mathbf{Z}/p\mathbf{Z})^*$ を位数が q となる元とし，$s \in \mathbf{Z}/q\mathbf{Z}$ をランダムに選び，$h = g^s \bmod p$ とする．また，関数 E, D を

$$E(m, r, g, h, p) = (g^r \bmod p, m \cdot h^r \bmod p) \quad (1)$$

$$D((x, y), s, p) = y \cdot x^{-s} \bmod p \quad (2)$$

とする．なお，関数 E の入力 r は $\mathbf{Z}/q\mathbf{Z}$ からランダムに選ばれた整数とする．すると，(g, h, p) を公開鍵，s を秘密鍵とし，暗号化関数を E，復号関数を D とすることにより，公開鍵暗号方式 (以下，方式 1) を構成できる．各設問に答えよ．

問 1 任意の $m \in (\mathbf{Z}/p\mathbf{Z})^*$，$r \in \mathbf{Z}/q\mathbf{Z}$ について，$D(E(m, r, g, h, p), s, p) = m$ となることを示せ．

問 2 $-1 \bmod p$ は，g が生成する $(\mathbf{Z}/p\mathbf{Z})^*$ の部分群 $\langle g \rangle$ に含まれていないことを示せ．

問 3 m の候補が $\{1, -1\}$ に限定されていたとする．すると，(m, r, g, h, p) を入力とする関数 E の出力 (x, y) のみが与えられたとき，s を利用することなく，m が 1 であるか -1 であるかを識別することができる．その方法を述べよ．

問 4 (g, g^x, g^y, g^z) が与えられたとき，$z = xy$ か，z が $\mathbf{Z}/q\mathbf{Z}$ からランダムに選ばれているかを判定する問題を DDH 問題という．m を $\langle g \rangle$ から選ぶことにより，DDH 問題が困難であるという仮定のもとで方式 1 は選択平文攻撃に対して識別不可能性を有していることが知られている．識別不可能性の定義を与えるとともに，このことを示せ．

Ⅷ経済

次の各語の意味するところについて、具体例を用いて、それぞれ20行程度（図表を含む）で説明せよ。

（1） アカロフ（G. Akerlof）の「レモン市場（market for lemons）」

（2） 不確実性下の意思決定問題における期待効用最大原理に関して生じる「アレー（M. Allais）のパラドックス」

Ⅸ経営

以下の問いに答えよ。

1．次の経営学者の業績を、10行以内で述べよ。
ポーター（M. E. Porter）

2．次の用語を、それぞれ5行以内で説明せよ。
執行役員制度、デリバティブ、発明報酬

X法律

グーグル社のストリートビュー*をめぐる法的問題点を複数取り上げ、自らの見解を述べよ。(六法使用可)

*グーグル社のストリートビューは、車上に 360 度カメラを搭載して街頭を走りながら連続的に撮影し、インターネット上で当該写真を公開するサービスである。利用者は、グーグル・マップを開き、任意の場所をクリックするか、住所を入力することによって、路上のパノラマ写真をあらゆる角度から閲覧することができる。