姓名＿＿＿＿＿＿

学籍番号＿＿＿＿＿＿

学部＿＿＿＿＿＿

クラス＿＿＿＿＿＿

科目番号＿＿＿＿＿＿

担当教員＿＿＿＿＿＿

装

订

线

大連理工大学

科目名：情報セキュリティ　問題種類：Pre　試験形式：開　巻

所属学部：国際情報ソフトウェア学部　試験の実施日：　年　月　日

問題用紙合計ページ数　5

注意：本当の試験は試験形式：　**閉**　です

	一	二	三	四							合計
配点	40	20	20	20							100
得点											

得点	

一、以下の各文章の空欄を埋めるのに適切な単語を解答欄に記せ。

1. 情報セキュリティで維持すべき基本的な三つの性質のうち、情報が許されたもののみに参照され、漏えいが防がれる性質のことを、（ア）と呼ぶ。情報が必要な場合に常に参照できるという性質のことを、（イ）と呼ぶ。また、情報の改ざんがないという性質のことを（ウ）と呼ぶ。
2. サーバに大量のリクエストを送りつけ、サーバの機能を停止させる攻撃のことを（エ）と呼ぶ。特に、Botnet などを用いて分散ネットワークを構成して攻撃するものを（オ）と呼ぶ。
3. 特定の ID に対し、可能性のあるパスワードを順に大量に試行することによって、その ID のパスワードを推測し、侵入する攻撃を（カ）と呼ぶ。
4. 共通鍵暗号方式では、送信者と受信者の間での鍵の受け渡しを安全に行うことが難しい。離れた二人の間で安全に鍵を交換するために考え出された、離散対数問題を用いた鍵交換プロトコルを（キ）と呼ぶ。
5. 平文と同じ長さの鍵との排他的論理和（exclusive-or）をとることによって暗号文を生成する方法のことを、（ク）と呼ぶ。平文を一定の bit の塊に分割して暗号化する方法のことは、（ケ）と呼ぶ。（ケ）のうち最もよく利用されていたのは DES であったが、これは日本の松井充によって開発された（コ）によって危殆化が深刻になり、米国（美国）では新たな（ケ）として（サ）が利用されることとなった。
6. 共通鍵暗号と公開鍵暗号について、一般的に暗号化や復号化の速度が速いのは（シ）である。
7. 公開鍵暗号方式では、各人が二つの鍵を生成し、お互いに利用する。A さんから B さんに通信する場合、通信文を暗号化して B さんにだけ届くようにするには、B さんの（ス）を用いて平文を暗号化する。B さんはこれによって暗号化された通信文を（セ）を用いて復号化できる。
8. ゼロ知識対話認証において 1 回の認証でウソが成立する確率は（ソ）である。

9. ハードウェアトークンや暗号表などをパスワードと併用して用いる認証方法を（ タ ）と呼ぶ。
10. 自己署名証明書、俗にいうオレオレ証明書は（ チ ）の可能性を排除できないために危険である。
11. NAT のうち IP アドレスの対応付けが静的なものを特に（ ツ ）と呼ぶ。
12. インターネットを利用した仮想的に専用線を構築する方法を（ テ ）と呼ぶ。（ テ ）のうち、ネットワーク層を用いたものに IPsec があるが、これは（ ト ）を通過できない可能性がある。
13. NIDS において不正な通信を検知する方法のひとつにデータ量が事前に設定された値よりも多い異常を検知する（ ナ ）がある。
14. SQL 文に不正な文字列を送り込むことによって攻撃する方法を（ ニ ）と呼ぶ。

解答欄：

ア		イ	
ウ		エ	
オ		カ	
キ		ク	
ケ		コ	
サ		シ	
ス		セ	
ソ		タ	
チ		ツ	
テ		ト	
ナ		ニ	

得点	

二、RSA 暗号に関する以下の問いに答えよ。余白には計算の途中結果を書き、最終的な計算結果を解答欄に記せ。

（１） N=10 を用いる RSA 暗号の公開鍵（N, e）と秘密鍵 d のペアを 1 組見つけよ。ただし、e≠d, e≠1, d≠1 となるように注意すること。

（２） （１）で求めた公開鍵を用いて、平文の値 3 を暗号化するとどのような値になるか求めよ。

（３） （２）で求めた暗号文を復号する方法を記せ。

解答欄：

(1)	e= d=	(2)		(3)	

DH鍵交換について、以下の問いに答えよ。
(1) Z mod 13 (整数を13で割ったあまりの集合)を求めよ
(2) 素数13に対する原始元を2とする。Aさんが乱数x=1、Bさんが乱数y=4を選んだとき、DH鍵交換で生成される共通鍵を求めよ。

解答欄：

(1) _____

(2) _____

得点	

三、以下の図 1 は Feistel 構造による暗号化方法を示している。以下の問題に答えよ。

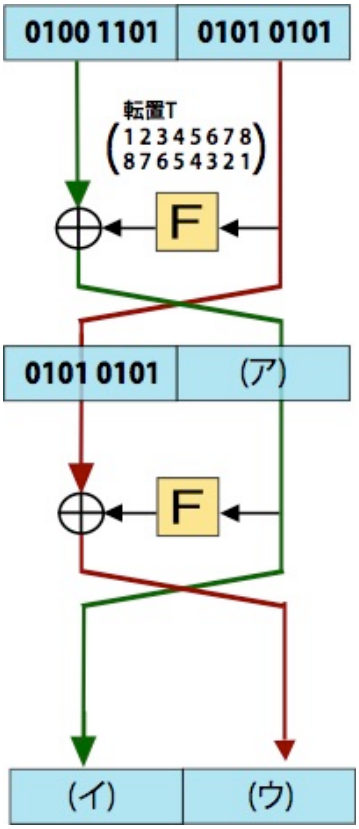

図 1

1. 図中にある⊕記号はある演算を示している。なんという演算か、漢字 6 文字で書け。

2. 次の空欄を埋めよ。かつて標準的なブロック暗号であった DES では、Feistel 構造においてラウンド関数 F に 8 つの［　　］ボックスと呼ばれる非線形のユニットがあった。

3. 1111 0000⊕0000 1111 を求めよ。

4. 0000 1111 を左に 2 ビット巡回シフトせよ。

5. 図 1 の空欄(ア)（イ）（ウ）を求めよ。なおラウンド関数は転置 T として、ビット列の前後を反転するものとする。(例：F(1001 0100) = 0010 1001)

解答欄：

1		2	
3		4	
4	（ア）		
	（イ）		
	（ウ）		