２．コンピュータの技術要素

２．３．　情報セキュリティ（ディジタル署名）

問題１

　共通鍵暗号方式に関する記述のうち、適切なものはどれか。

ア：　暗号化に用いる鍵を第三者に公開しても、第三者は暗号文を複合できない。

イ：　公開鍵暗号方式よりも、暗号化処理と複合処理の計算量は少ない。

ウ：　通信経路で改ざんされた暗号文を複合処理で訂正し、元の暗号文に復元する機能を持つ。

エ：　複数の相手ごとに通信内容を秘密にしたい場合でも、暗号化に用いる鍵は一つである。

問題２

　無線LANで利用される暗号方式の規格はどれか。

ア：　AES

イ：　DES  
ウ：　RSA

エ：　WPA2

問題３

　Xさんは、Yさんにインターネットを使って電子メールとしている。電子メールの内容を秘密にする必要があるので、公開鍵暗号方式を用いて、暗号化して送信したい。電子メールの内容を暗号化するのに使用する鍵はどれか。

ア：　Xさんの公開鍵

イ：　Xさんの秘密鍵

ウ：　Yさんの公開鍵

エ：　Yさんの秘密鍵

問題４

　公開鍵基板（PKI）において認証局（CA）が果たす役割はどれか。

ア：　SSLを利用した暗号化通信で使用する認証プログラムを提供する。

イ：　Webサーバに不正な仕組みがないことを示す証明書を発行する。

ウ：　公開鍵が非人称者のものであることを示す証明書を発行する。

エ：　非人称者のディジタル署名を安全に送信する。

問題５

セッション鍵暗号方式で用いられるハイブリッド方式に関する記述のうち、適切なものはどれか。

ア：　共通鍵と公開鍵で二重に暗号化するので改ざんが難しい。

イ：　共通鍵と公開鍵を併用するので、高速な暗号通信には向かない。

ウ：　公開鍵暗号方式を使って、共通鍵を暗号化して通信相手に送信する。

エ：　使用する鍵の数は、全体で単独方式の2乗倍必要になる。

問題６

　受信した電子メールにPKI（公開鍵基盤）を利用したディジタル署名を付与した場合に関する記述ａからｄのうち、判断可能な記述だけをすべて挙げらられたものはどれか。

ａ　電子メールの添付ファイルはウィルスに感染していない。

ｂ　電子メールの内容は通信途中において、他の誰にも盗み見られていない。

ｃ　電子メールの発信者は、なりすましされていない。

ｄ　電子メールは、通信途中で改ざんされていない。

ア：　ａ，ｂ

イ：　ａ，ｃ

ウ：　ｂ，ｄ

エ：　ｃ，ｄ

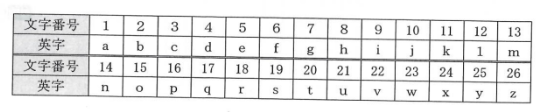
問題７

　小文字の英字からなる文字列の暗号化を考える。次表で英字を文字番号に変換し、返還後の文字番号について1文字目には１を、２文字目には２を、・・・、ｎ文字目にはｎを加える。それぞれの数を26で割った余りを新たに文字番号とみなし､表から対応する英字に変換する｡

例) fax → 6,　1,　24 → 6+1,　1+2,　24+3

→ 7,　3,　27 → gca

この手続きで暗号化した結果が､“tmb”であるとき､元の文字列はどれか｡



ア：　she

イ：　shy

ウ：　ski

エ：　sky

２．コンピュータの技術要素

２．３．　情報セキュリティ（ディジタル署名）

問題１【解答：イ】

ア：　共通鍵暗号方式は、暗号化と復号に同じ鍵（共通鍵）を使用する方式なので、暗号化に用いた鍵を第三者に公開すると、第三者は暗号文を復号できる。

イ：　共通鍵暗号方式は、送信者と受信者しか鍵を知らない為、暗号化／復号の処理が簡単（少ない計算量）で、暗号通信を高速に行える。（正解）

ウ：　暗号方式は、第三者に盗聴されるのを防ぐ技術であるため、改ざんされた暗号文を訂正して元の暗号文に復号する機能はない。

エ：　共通鍵暗号方式は、通信相手ごとに鍵を用意しなければいけない。

問題２【解答：エ】

・ＡＥＳ（Advanced Encryption Standard）

：ラインダール（Rijndael）法を利用した共通鍵暗号方式である。

・ＤＥＳ（Data Encryption Standard）

：ブロック暗号を利用した共通鍵暗号方式である。

・ＲＳＡ（Rivest, Shamir, Adleman）

：非常に大きな数の素因数分解を利用した公開鍵暗号方式である。

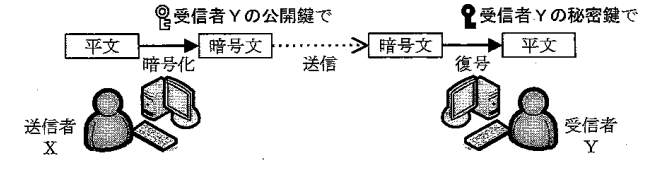
・ＷＰＡ２（Wi-Fi Protected Access 2）

：共通鍵暗号方式（AES）を使用した、無線LANの暗号方式の規格である。（正解）

問題３【解答：ウ】

　公開鍵暗号方式は、暗号化のカギを公開（公開鍵）し、復号に使うカギを秘密（秘密鍵）にする方法である。暗号化のカギを公開しているので、暗号化の処理は複雑にしなければいけないが、一組の鍵で多数の人と暗号通信を行えるので、鍵の管理が簡単である。

　図に示すように、Xさんが公開鍵暗号方式を用いてインターネット経由でYさんに電子メールを送るとき、電子メールの内容を暗号化するのに使用する鍵は「Yさんの公開鍵」である。



問題４【解答：ウ】

　公開鍵基盤（PKI：Public Key Infrastructure）とは、公開鍵暗号方式やディジタル署名を利用したセキュリティ環境のことである。公開鍵基盤（PKI）でも公開鍵の正当性を確認するために、認証局（CA：Certification Authority）のディジタル証明書が利用される。したがって、公開鍵基盤（PKI）において認証局（CA）が果たす役割は「公開鍵が被認証者のものであることを示す証明書を発行する」ことである。

問題５【解答：】

問題６【解答：】

問題７【解答：】

問題８【解答：】