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

問題７