2006年度

問6.自信なし

family , type , protocol , socket の4つの引き数のことか？？？

問7.公開鍵暗号をそれ以前の秘密鍵暗号(共通鍵暗号)と対比させることがポイントと思われる。

【動作原理】

公開鍵暗号では暗号化に使う鍵と復号に使う鍵が分離されており、暗号化に使った鍵で復号を行うことはできず、片方からもう一方を割り出すことも容易にはできないようになっている。鍵の持ち主は復号に使う鍵のみを他人に知られないように管理し、暗号化に使う鍵は公開する。公開鍵暗号で秘密のメッセージを送受信する場合、送信者は受信者が公開している公開鍵を入手して暗号化を行う。暗号化されたメッセージは受信者の持つ秘密鍵でしか復号できないため、途中で第三者に傍受されても中身を解読されることはない。

【特徴】

公開鍵暗号では暗号に使う公開鍵は第三者に知られても解読されないため、鍵の安全な輸送が必要なく、安全性も高い。公開鍵暗号は秘密鍵暗号暗号化と復号に同じ鍵を用いる暗号方式。暗号文の送信者と受信者で同じ鍵を共有する必要があり、暗号文を送受信する前にあらかじめ安全な経路を使って秘密の鍵を共有する必..よりも処理が複雑になりがちであり、より多くの計算資源や時間を必要とする。このため、暗号通信に利用する場合は、実際の通信内容の暗号化には即興で鍵を生成した秘密鍵暗号を使い、その鍵を送信者と受信者の間で安全に交換するために公開鍵暗号を使うといった使い方をすることが多い。

問8.スケールアップ・スケールアウトの問題。問題文で聞かれているのは、スケールアウトの方法を3つ答えよ、ということだと思われる。

①ウェブサーバファームとして使用されているラックマウントサーバ群にサーバを追加する。

②ブレードサーバにブレードを追加する。

③サーバの仮想化機能を使って、ひとつの筐体内で仮想的に複数サーバを構築する。(スケールウィズインもしくは仮想スケールアウトという)