SECURITY-Prüfung am 30.1.2004

Name:_____ Matr.Nr.: _____ Kennzahl: ___

1. Abstrahlung eines PCs:
Warum kann ein PC mit einem herkömmlichen Bildschirm (CRT) mehrere Räume entfernt oder von der Strasse aus mit einer relativ einfachen Ausrüstung abgehört werden und warum ist das am Abhörgerät dargestellte Bild relativ gut leserlich?
a) weil am abzuhörenden PC der Phosphor des Bildschirmes gut nachleuchtet
b) weil das Bild am abzuhörenden PC mindestens 50 mal pro Sekunde am Bildschirm wiederholt dargestellt wird
c) weil jedes am Bildschirm dargestellte Zeichen aus vielen einzelnen Punkten aufgebaut ist
d) weil der Bildschirm die Auflösung eines TV-Gerätes aufweist und daher das Bild auf einem TV-Gerät einfach abgebildet werden kann

2. Welche angegebenen Komponenten gehören sicher zu einer heute im Einsatz befindlichen Chipkarte:
a) Plastikkarte
b) Mikroprozessor
c) Lautsprecher
d) Mini-Kamera
e) EEPROM-Speicher

3. Welche angegebenen biometrischen Daten sind NICHT im praktischen Einsatz?
a) Fingerabdruck
b) Iris-Scan
c) Digitale Signatur
d) Fußabdruck des rechten Fußes
e) Handflächenabdruck, Eingabe mit gespreizten Fingern

4. Welche Kennwerte (Leistungsmerkmale) sind bei biometrischen Daten besonders wichtig und werden auch bei der Ermittlung der Gleichfehlerrate benötigt?
a) wie leicht kann die Eingabe beobachtet werden
b) wie viele Daten werden bei der Merkmalsextraktion weggeworfen
c) wie viele berechtigte Personen werden abgelehnt
d) wie oft müssen bei der Ersteingabe (für den späteren Vergleich) biometrische Daten eingegeben werden
e) wie viele unberechtigte Personen werden zugelassen

5. Was sind üblicherweise Vorteile von Passwörtern?
a) es kann jederzeit geändert werden
b) man muss sich das Passwort merken
c) man kann es frei wählen
d) es kann bei der Eingabe beobachtet werden
e) mit der Passworteingabe gibt man eine Willenserklärung ab

6. Welche angegebenen Schutzmethoden sind für den Softwareschutz vor Raubkopien geeignet?
a) Virenschutzprogramm
b) Dongle
c) Service (Hotline, Updates etc.)
d) Computerzeitmessgerät
e) Ständige Darstellung des Namens des SW-Lizenznehmers am Bildschirm

7. Wie kann man sich herkömmliche, sichere Passwörter leichter merken?
a) Durch Einbau von Rechtschreibfehlern in das Passwort
b) Durch Codierung von Daten aus dem aktuellen Sport
c) Durch Verwendung von Namen von engen Verwandten

8. Welche nachfolgend angegebenen Personengruppen sind ohne IT-Sicherheitsmaßnahmen für die IT-Sicherheit eines Unternehmens gefährlich?
a) Wartungstechniker
b) EDV-Leiter
c) Geschäftsführer
d) Sicherheitsbeauftragte
e) Gekündigter Mitarbeiter
f) Putzdienst

9. Ein in Word verfasstes Dokument wurde nur mit einer digitalen Signatur versehen und so an den Empfänger per Internet übertragen. Der Empfänger überprüft nun die Signatur. Welche Schritte werden dabei auf Empfängerseite unter anderem durchgeführt (welche unten angegebenen Schritte sind dabei richtig)?
a) zuerst wird das Dokument mit dem geheimen Schlüssel entschlüsselt
b) zuerst wird das Dokument mit dem öffentlichen Schlüssel entschlüsselt
c) zuerst wird das Dokument mit einer Hashfunktion entkomprimiert
d) zuerst wir das Dokument mit einer Hashfunktion komprimiert
e) dann wird das Dokument verschlüsselt
f) dann wird die mitübertragene Signatur mit dem geheimen Schlüssel entschlüsselt
g) dann wird die mitübertragene Signatur mit dem öffentlichen Schlüssel entschlüsselt
h) dann wird das Ergebnis der Hashfunktion mit dem geheimen Schlüssel entschlüsselt
i) dann wird das Ergebnis der Hashfunktion mit dem öffentlichen Schlüssel entschlüsselt
j) zuletzt werden zwei der oben angegebenen Ergebnisse verglichen

10. Welche unten angegebenen Speichergrößen für die Daten sind bei heutigen Chipkarten (Norm ISO 7816) mit Mikroprozessor möglich und üblich
a) 4 KB
b) 32 KB
c) 4 MB
d) 64 MB

11. Wie lange müssen Schlüssel für die symmetrische Kryptografie sein, damit sie aus heutiger Sicht sicher sind, und wie kann man die Sicherheit bei der symmetrischen Verschlüsselung bei herkömmlichen Verfahren (DES, IDEA etc.) verbessern?
a) 56 Bit
b) 128 Bit
c) durch mehrfache Verschlüsselung hintereinander
d) durch zuerst verschlüsseln, dann entschlüsseln und dann wieder verschlüsseln
e) durch eine Rückkoppelung (XOR-Verknüpfung) des (n-1)-ten verschlüsselten Blockes mit dem n-ten unverschlüsselten Blocks

12. Bei welchen Zertifizierungen handelt es sich um KEINE international anerkannten Sicherheitszertifizierungen?
a) ITSEC E2
b) ÖNORM H14
c) Common Criteria EAL4
d) Red Book DG 27