Sommersemester 2005

Hasso- Plattner- Institut, Universität Potsdam

Übung zur Vorlesung

Fachgebiet Internet- Technologien und - Systeme

Meinel / Kutzner

Übersichts- Aufgabenblatt

Dieses Aufgabenblatt dient zur Nachbearbeitung des in dieser Vorlesung vermittelten Stoffes. Eine Abgabe bzw. Bewertung der Antworten erfolgt nicht.

1. Welche Sicherheitsanforderungen können in der Datenkommunikation notwendig sein? Erläutern Sie diese an Beispielen.

2. Was ist ein Kommunikationsprotokoll, was ist ein Krypto- Protokoll? Geben Sie jeweils ein einfaches Beispiel an. Welche Eigenschaften können Krypto- Protokolle haben und wie sehen Angriffe auf sie aus?

3. Was versteht man unter einem Experiment, Elementarereignis und einem Ereignisraum in der Wahrscheinlichkeitstheorie? Wie berechnet sich die bedingte Wahrscheinlichkeit?

4. Was versteht man unter der Entropie in der Informationstheorie?

5. Welches Ziel verfolgt die Komplexitätstheorie? Wozu dienen die Mengen O, Ω und Θ? Wie werden sie definiert?

6. Wie sind die Komplexitätsklassen N, NP und NPC definiert? Welche Rolle spielen sie in der Kryptographie?

7. Was sagt der Fundamentalsatz der Zahlentheorie aus? Wie lautet die Eulersche Phi-Funktion? Wie bestimmt man größten gemeinsamen Teiler mit dem euklidischen Algorithmus?

8. Was sind Kongruenzklassen? Wie ist Z_n definiert und welche Eigenschaften hat diese Menge?

9. Definieren Sie Z_n^*. Was sagen die Theoreme von Euler und Fermat aus? Wie ist die Ordnung definiert? Was ist ein Generator?

10. Welche Eigenschaften müssen Gruppen erfüllen? Wie definieren sich Ringe und Körper? Geben Sie jeweils ein Beispiel an. Wann spricht man von Polynomringen und wann von endlichen Körpern?

11. Welche Berechnungsprobleme stecken hinter SUBSET- SUM, FACTORING, RSAP, SQROOT, DLP und DHP?

12. Welche Grundidee steckt hinter probabilistischen Primzahlentests? Wie funktionieren die Primzahlentests von Fermat, Solovay- Strassen und Miller- Rabin?

13. Was sind Pseudozufallsgeneratoren?

14. Was versteht man unter symmetrischer und asymmetrischer Verschlüsselung? Geben Sie Algorithmen an, die diesem Prinzip entsprechen. Welche Vor- und Nachteile haben beide Verschlüsselungsverfahren? Wie unterscheiden sich Public- und Secret- Key Verfahren?

15. Welche Angriffe sind auf Krypto- Systeme möglich? Wann gilt ein Krypto- System als sicher? Was versteht man unter dem Kerckhoff- Prinzip?

Bitte wenden!

16. Geben Sie Beispiele für Substitutions- Chiffren an. Auf welchem Prinzip basieren sie? Was sind polyalphabetische Chiffren? Welche Beispiele dafür kennen Sie?

17. Wie funktioniert der Data Encryption Standard (DES)? Welche mathematischen Verfahren spielen hier eine Rolle? Was versteht man unter Triple- DES?

18. Was ist IDEA? Wie ist die Funktionsweise des Advanced Encryption Standard (AES)?

19. Beschreiben Sie den Diffie- Hellman- Schlüsselaustausch. Wie funktioniert das RSA Krypto- Verfahren? Auf welcher Grundidee basiert die Elliptic Curve Cryptography?

20. Was ist die Aufgabe einer Hash- Funktion? Welche Bedeutung hat sie in der Informationssicherheit? Nennen Sie die Anforderungen, die an eine Hash- Funktion gestellt werden. Was versteht man unter den Begriffen „kollisionsfrei“ und „Einweg- Funktion“? Was ist das Ziel von Angriffen?

21. Wie ist die Funktionsweise von SHA- 1? Welche Operationen werden angewendet? Wie unterscheiden sich MD4 und MD5 von SHA- 1? Was können Sie zur Sicherheit dieser Verfahren sagen?

22. Wie unterscheiden sich symmetrische und asymmetrische Verschlüsselungsprotokolle? Welche Vor- und Nachteile haben sie? Warum verwendet man hybride Verschlüsselungsprotokolle?

23. Wozu dienen digitale Signaturen? Wie werden Public- Key Krypto- Systeme zum Signieren verwendet? Wie kann der Rechenaufwand für das Signieren großer Nachrichten verringert werden?

24. Wie werden Signaturen mit RSA, ElGamal und DSS erzeugt? Auf welcher Idee beruhen Einmal- Signaturen? Welche Angriffe sind auf Signaturen möglich?

25. Was versteht man unter Authentifikation? In welche drei Bereiche lassen sich Authentifikationsverfahren unterteilen? Wie erfolgt die Authentifikation mittels Passwörtern? Wie funktionieren Challenge- Response- Protokolle? Was ist ein Smart Token?

26. Beschreiben Sie, wie die Authentifikationsprotokolle nach Schnorr, Zero- Knowledge und nach Fiat- Shamir funktionieren.

27. Wie sieht der Lebenszyklus eines Schlüssels aus? Welche Aufgaben umfasst das Schlüsselmanagement? Was versteht man unter Session Keys? Erklären Sie kurz die Schlüsselverteilung nach Blom.

28. Wie erfolgt die Schlüsselvereinbarung bei Diffie- Hellman, im Station- to- Station- Protokoll, bei MTI und nach Girault?

29. Wozu dienen PKIs? Welche Vertrauensmodelle gibt es? Aus welchen Komponenten bestehen PKIs bzw. Trust Center? Wozu dient das Zertifikate- Management? Was versteht man unter Enrollment? Wozu dient eine Certificate Policy? Welche wichtigen PKI- Standards gibt es?

30. Wozu dienen Verzeichnisdienste? Welche wichtigen Standards existieren für Verzeichnisdienste? Welche Verfahren gibt es, um PKI- Teilnehmer über gesperrte Zertifikate zu informieren?

31. Was ist IPSec? Wozu dient SSL? Welche Aufgaben erfüllt PGP?