Übung zur Vorlesung

Kryptographie und Komplexität

Prof. Dr. Christoph Kreitz
Universität Potsdam, Theoretische Informatik, WS 2015/16

Blatt 5 — Besprechungstermin: —

Die folgenden Fragen sind typische Fragen, die während einer Prüfung zur Kryptographie und Komplexität gestellt werden könnten. Die Sammlung erhebt keinen Anspruch auf Vollsständigkeit und geht im Gesamtumfang natürlich weit über den einer Prüfung hinaus.

Aufgabe 5.1 (Einfache kryptographische Systeme und ihre Analyse)

1. Was sind die Grundbestandteile eines Kryptosystems?
2. Nennen Sie die wichtigsten einfachen Verschlüsselungsverfahren
3. Welche grundsätzlichen Arten der Kryptoanalyse gibt es?
4. Erklären Sie den Verschiebungschiffre
   Welche Attacken sind möglich und wie schnell kann ein Schlüssel gefunden werden?
5. Erklären Sie den Affin-linearen Chiffre
   Welche Attacken sind möglich und wie schnell kann ein Schlüssel gefunden werden?
6. Erklären Sie den Substitutionschiffre
   Welche Attacken sind möglich und wie schnell kann ein Schlüssel gefunden werden?
7. Erklären Sie den Vigenere Chiffre
   Welche Attacken sind möglich und wie schnell kann ein Schlüssel gefunden werden?
8. Erklären Sie den Hill Chiffre
   Welche Attacken sind möglich und wie schnell kann ein Schlüssel gefunden werden?
9. Erklären Sie den Permutationschiffre
   Welche Attacken sind möglich und wie schnell kann ein Schlüssel gefunden werden?
10. Erklären Sie die Vorgehensweise von Stromchiffren
    Welche Attacken sind möglich und wie schnell kann ein Schlüssel gefunden werden?
11. Was sind die Grundbestandteile eines Kryptosystems?
12. Welche Arten von Sicherheitsanforderungen kann man stellen
13. Erklären Sie, wie man die Analyse *bedingter Wahrscheinlichkeiten* dazu verwenden kann, Geheimnachrichten zu entziffern.
14. Erklären Sie den Unterschied zwischen berechenbarer Sicherheit, beweisbarer Sicherheit und unbedingter/perfekter Sicherheit
15. Unter welchen Voraussetzungen ist perfekte Sicherheit erreichbar?
16. Was ist ein One-Time Pad und wann kann es perfekte Sicherheit garantieren? Was sind die Nachteile?
17. Was ist eine Einwegfunktion?
18. *aus der Mathematik*:

    Wieviele zu n teilerfremde Zahlen gibt es in der Gruppe $\mathbb{Z}_n$?

    Was besagt der Satz von Bayes und wozu braucht man ihn?

Aufgabe 5.2 (Substitutions-/Permutationsnetzwerke, DES & AES)

1. Was ist eine Produktchiffre?
2. Welche Eigenschaften sollte eine Produktchiffre nicht besitzen?
3. Erklären Sie den Unterschied zwischen Konfusion und Diffusion einer Chiffrierung.
4. Was ist ein Substitutions-/Permutationsnetzwerk?
   Erklären sie die Arbeitsweise und die dafür notwendigen Begriffe
5. Wie funktioniert eine lineare Attacke?
6. Wie funktioniert eine differentielle Attacke?
7. Erklären Sie den grundsätzlichen Aufbau des DES
   Beschreiben Sie dazu (grob) die wesentlichen Komponenten des Verschlüsselungsalgorithmus und der Schlüsselerzeugung.

   Welche Attacken sind heutzutage erfolgreich?
8. Erklären Sie den grundsätzlichen Aufbau des AES.
   Beschreiben Sie dazu (grob) die wesentlichen Komponenten des Verschlüsselungsalgorithmus und der Schlüsselerzeugung.

Aufgabe 5.3 (Public-key Kryptographie mit RSA)

1. Erklären Sie den Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung
2. Erklären Sie das Verfahren der Public-key Kryptographie mit dem RSA Schema.
3. Wie wird konkret im RSA Verfahren ver- und entschlüsselt? Warum funktioniert das?

   Gehen Sie dabei unter anderem auf die folgenden Aspekte ein:
   (1) Gesamtszenario des Verfahrens,
   (2) Konkrete Ver-/Entschlüsselungsfunktionen,
   (3) Bestimmung der Schlüssel
   (4) Begründung der Korrektheit,
   (5) Berechnungsaufwand für Ver-/Entschlüsselung,
   (6) Sicherheit (welches Problem ist zu lösen, um das Verfahren zu brechen / Aufwand dafür?).
4. Wie werden Schlüssel für das RSA Verfahren bestimmt?
5. Wie groß ist die Komplexität der Verschlüsselung, Entschlüsselung, Schlüsselbestimmung ?
6. Worauf basiert die Sicherheit von RSA?
   Welches Problem ist zu lösen, um das Verfahren zu brechen? Was ist der Aufwand dafür?
7. Beschreiben Sie mögliche Schwächen von RSA.
8. Auf welche Art kann das RSA Verfahren semantisch sicherer gemacht werden?
9. Was besagt der chinesische Restsatz und wozu kann man ihn gebrauchen?
10. Bestimmen Sie eine Zahl x mit $x \equiv 17 \bmod 89$ und $x \equiv 7 \bmod 47$
11. Was bestimmt die Euler'sche φ Funktion?
12. Was besagt der kleine Satz von Fermat?

Aufgabe 5.4 (Primzahltests und Faktorisierung)

1. Wozu werden Primzahltests benötigt?
2. Nennen Sie die gängigsten Testverfahren für Primzahlen.
   Welche Komplexität haben diese Verfahren?

3. Beschreiben Sie den Primzahltest von Solovay-Strassen. Geben Sie dabei auch eine grobe Begründung der Korrektheit, eine Laufzeitanalyse und die Fehlerwahrscheinlichkeit der Aussage “p ist Primzahl” an.
4. Beschreiben Sie den Primzahltest von Miller-Rabin. Geben Sie dabei auch eine grobe Begründung der Korrektheit, eine Laufzeitanalyse und die Fehlerwahrscheinlichkeit der Aussage “p ist Primzahl” an.
5. Warum ist das Miller-rabin Verfahren trotz gleicher Komplexität besser als Solovay-Strassen?
6. Wozu werden Faktorisierungsalgorithmen benötigt?

   Warum ist es gut, daß alle bekannten Verfahren NICHT polynomiell arbeiten?
7. Beschreiben Sie die gängigsten Faktorisierungsalgorithmen und ihre Komplexität.
8. Beschreiben Sie den Pollard $p-1$ Algorithmus und begründen Sie seine Korrektheit.
9. Was ist die Schlüsselidee des Pollard ρ Algorithmus?

Aufgabe 5.5 (ElGamal Systeme)

1. Was ist das Problem der diskreten Logarithmen?
2. Wie kann mit dem Diffie-Hellman Verfahren ein gemeinsamer Schlüssel erzeugt werden ohne daß eine Partei alles weiß?
3. Beschreiben Sie die Arbeitsweise des ElGamal Systems (Ver-, Entschlüsselung, Nachweis, daß es funktioniert, Komplexität)
4. Wie kann man effizient ver- und entschlüsseln?
5. Was ist nötig, um das Verfahren zu brechen und wie aufwendig ist das ?
6. Welche Verfahren zur Berechnung diskreter Logarithmen gibt es
7. Beschreiben Sie den Shank’schen Algorithmus (inkl. Korrektheitsbegründung und Komplexität)
8. Beschreiben Sie (grob) den Pollard ρ Algorithmus (inkl. Korrektheitsbegründung und Komplexität)
9. Beschreiben Sie (grob) das Pohlig-Hellmann Verfahren (inkl. Korrektheitsbegründung und Komplexität)
10. Beschreiben Sie die Kernideen der Index-Calculus Methode für Z_p (inkl. Komplexität und einer Oberflächlichen Korrektheitsbegründung)
11. Warum betrachtet man diskreten Logarithmen über endlichen Körpern anstelle von $\mathbb{Z}_n$?
12. Durch welche Gleichung werden elliptische Kurven definiert und welche Randbedingungen müssen erfüllt sein?
13. Wie kann man elliptische Kurven als Gruppe beschreiben, um das Problem der diskreten Logarithmen anzugehen?
    Beschreiben Sie die wichtigsten Gruppenoperationen graphisch bzw als Formeln

    Bestimmen Sie das Inverse des Punktes (3,8) auf der Elliptischen Kurve $E(23, 2, 8)$.
14. Wieviele Punkte kann eine Elliptische Kurve über $\mathbb{Z}_{8069}$ minimal und maximal haben (eine grobe Schätzung reicht)?
15. Wozu benutzt man elliptische Kurven in der Kryptographie?
16. Was ist der Vorteil von Verschlüsselung mit elliptischen Kurven gegenüber RSA?
17. Warum ist das Problem der diskreten Logarithmen für elliptischen Kurven schwerer zu brechen als über $\mathbb{Z}_n$

    Was ist das beste hierfür bekannte Lösungsverfahren?
18. Es ist bekannt, daß alle Elliptische Kurven isomorph zu einer Gruppe der Form $\mathbb{Z}_m \times \mathbb{Z}_n$ sind. Warum kann diese Isomorphie nicht dazu verwendet werden, um das Problem des diskreten Logarithmus für elliptische Kurven genauso effizient zu lösen wie für $\mathbb{Z}_m \times \mathbb{Z}_n$?
19. Konkret: was muß beim Schlüsselaustausch übermittelt werden?

Aufgabe 5.6 (Anwendungen)

1. Welche Sicherheitsziele werden durch die Verwendung von
   (1) kryptographischen Hashfunktionen, (2) Message Authentication Codes,
   (3) digitalen Signaturen, (4) Passwörtern und (5) Secret-Sharing Protokollen angesprochen?
2. Nennen Sie drei wichtige Sicherheitsanforderungen an kryptographische Hashfunktionen.
3. Was ist eine (keyed) Hashfamilie und wozu wird dieses Konzept gebraucht?
4. Erklären Sie die 3 Sicherheitsprobleme für Hashfunktionen und den Zusammenhang zwischen ihnen
5. Was besagt das Geburtstagsparadox?
6. Was ist der Grundaufbau iterierter Hashfunktionen und wozu dienen sie?
7. Erklären Sie die Merkle-Damgard Konstruktion
8. Wie funktioniert SHA-1 und welche Attacken sind möglich
9. Was ist ein Message Authentication Code und wozu dient er?
   Erklären Sie die grundsätzliche Vorgehensweise und ihre Anwendung
10. Was ist ein (ε, q)-Forger? (Fälscher)
11. Wozu braucht man Digitale Unterschriften
12. Wie arbeitet ein Signatursystem intuitiv?
    Was sind seine Komponenten
13. Welche Arten möglicher Fälschungen gibt es
14. Wie kann man digitale Unterschriften mit RSA generieren?

    Welche Attacken auf diese Signaturen sind möglich ?
15. Warum kann man Polynome als Schwellenschemata zur Verteilung von Geheimnissen auf n Personen mit Schwelle t verwenden?
16. Was ist das Ziel anonymer Vergleichsprotokolle? Wozu kann man diese verwenden?
17. Was ist der Unterschied zwischen elektronischem Bargeld und EC mit Bankkarten?
18. Nennen Sie wichtige Anforderungen an Online-Voting.
19. Nennen mögliche Vorteile und Gefahren von Car-2-Car Kommunikation.