Einführung Kryptographie und IT-Sicherheit

Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

June 1st, 2020

Montag 1. Juni, 13:15

Fragen zum Skriptum - Abschnitt 3.4.1 - 3.4.4

1. Erklären sie wie das Knapsack Problem verwendet wird um ein public-key System mit Ver- und Entschlüsselung zu definieren.
2. Erklären sie warum und wie das “einfache” Knapsack Problem gelöst werden kann.
3. Was ist die Grundidee des Merkle-Hellman Algorithmus ?
4. Wie steht es um die Sicherheit der Knapsack-basierten Verschlüsselungsverfahren ?
5. *** Rechnen sie ein konkretes Zahlen-Bsp. für den Rabin Algorithmus durch und illustrieren/erklären sie warum die Entschlüsselung ohne Kenntnis von p und q schwierig ist. ***
6. *** Leiten sie die angegebenen Lösungen für den Rabin Algorithmus her. ***
7. Welche Rolle spielt der Parameter K im El Gamal Algorithmus ?

Montag 1. Juni, 13:15

Fragen zum Skriptum - Abschnitt 3.4.4 - 3.5.2

8. *** Beweisen sie die Bedingung für die El Gamal Unterschriftsverifikation und erklären sie warum ein Angreifer das diskrete Logarithmenproblem lösen müsste (Achtung: wie bei RSA sind hier verschiedenen Restklassenkörper involviert !) ***
9. Erklären sie die Korrektheit der angegebenen El Gamal Entschlüsslungsformel und erklären sie warum ein Angreifer das diskrete Logarithmenproblem lösen müsste.
10. Was sind die fundamentalen Unterschiede zwischen El Gamal und DSA ?
11. Vergleichen sie RSA und DSA im Kontext mit digitalem Signieren.
12. Was ist die Motivation für ein Zero-Knowledge Protokoll ?
13. Erklären sie das Ali Baba Zero-Knowledge Protokoll.
14. Erklären sie das vereinfachte Feige-Fiat-Schamir Protokoll.

Montag 1. Juni, 13:15

Fragen zum Skriptum - Abschnitt 3.5.2

15 *** Rechnen sie ein Zahlen Beispiel für das vereinfachte Feige-Fiat-Schamir Protokoll durch (alle Fälle für b) und erklären sie inwieweit die zero-knowledge Eigenschaft erfüllt ist, obwohl im Fall $b = 1$ der Wert von s in der geschickten Nachricht enthalten ist. ***

16 Wie kann Peggy im Fall von $b = 1$ trotzdem eine Täuschung vornehmen ? Was bedeutet das für den Fall $b = 0$?

17 Erklären sie den (etwas komplizierteren) tatsächlichen Algorithmus.

18 Erklären sie den Protokollablauf des Diffie-Hellman Key Exchange Verfahrens für zwei und drei TeilnehmerInnen.

19 Warum ist es wichtig dass im Diffie-Hellman Key Exchange g eine Primitivwurzel ist ?

20 Woher haben “Elliptic Curve Crypto Systems” ihren Namen ? Was ist deren Anwendungsgebiet ?

Montag 1. Juni, 13:15

Fragen zum Skriptum - Abschnitt

21. Wie sieht Diffie-Hellman Key Exchange auf Elliptischen Kurven aus ? Was macht man mit den erhaltenen Punkt Koordinaten ?
22. Motivieren sie den Einsatz von Probabilistischer Kryptographie. Bei welchem Verfahren ist dies bisher schon vorgekommen ?
23. *** Was bedeutet IND-CPA Sicherheit und welche der besprochenen Verfahren sind (nicht) IND-CPA sicher ? ***
24. *** Rechnen sie ein Zahlenbeispiel für Verschlüsselung mit dem Blum-Blum-Shub OTP durch und erklären sie warum das sicher ist (was ein Angreifer tun müsste um das Verfahren zu brechen). ***
25. Erklären sie die Anwendung von Quantenprinzipien auf das besprochene Key-exchange Verfahren.
26. Wie funktioniert bei diesem Ansatz die Intrusion Detection ?
27. Vergleichen sie den Sicherheitsbegriff der Key-Exchange Verfahren: Diffie-Hellman vs. Quantenkryptographie.