Einführung Kryptographie und IT-Sicherheit

Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

April 20th, 2020

Fragen zum Skriptum - Abschnitt 1.3.3.4 - 1.3.3.5

1. Wie funktioniert eine digitale Empfangsbestätigung unter Verwendung von public-key Kryptographie ?
2. ** Eklären sie die beschriebene Protokollattacke gegen public-key digitale Empfangsbestätigungen und machen sie explizit, inwiefern die Vorraussetzung $V_x = E_x$ und $S_x = D_x$ für den Angriff wesentlich ist (bzw. zeigen sie woran der Angriff scheitert wenn diese Bedingungen nicht erfüllt sind). **
3. Welche zusätzliche Annahme muss man für einen erfolgreichen Angriff treffen ?
4. ** Kann durch die Verwendung von One-Way Hash Funktionen bei den Unterschriften dieser Angriff verhindert werden, selbst wenn obige Vorraussetzung erfüllt ist ? Erklären sie das ! **
5. Erklären sie die Durchführung eines Schlüsselaustauschs mit Hilfe von Symmetrischer Kryptographie und die Schwäche(n) dieses Ansatzes.

Montag 20 April, 13:15

Fragen zum Skriptum - Abschnitt 1.3.3.6 - 1.3.3.7

6. Erklären sie den “Man in the Middle” Angriff. In welchen Zusammenhang steht dieser mit bereits diskutierten problemen bei der public-key Kryptographie ?
7. Erklären sie das Interlock Protokoll - was ist wesentliche Vorraussetzung bei einem entsprechenden Block Algorithmus ?
8. Wie könnte ein Angreifer das Interlock Protokoll “aushebeln” wenn er den ersten Teil der Nachrichten nicht entschlüsslen kann ? Ist das realistisch ?
9. Wie funktioniert die klassische PWD-basierte Authentifizierung auf einem Computer ? Warum werden die PWD nicht in Plaintext gespreichert ?
10. Was ist eine Dictionary Attack ? warum ist daher die Passwort-Wahl wesentlich ?
11. Was ist “Salt” ? Warum wirkt es gegen Dictionary Angriffe ?

Montag 20 April, 13:15

Fragen zum Skriptum - Abschnitt 1.3.3.7 - 1.3.3.10

12. Erklären sie SKEY Authentifizierung - inwiefern unterschiedet sich das von vielen TAN Systemen ?
13. Erklären sie den beschriebenen Ansatz zur Authentifizierung mit public key Verfahren.
14. Warum ist es unsicher irgendwelche “zufälligen” Strings mit dem private Key zu verschlüsseln ?
15. Wird bei multiple key public key Kryptographie eine Nachricht mit einer bestimmten Schlüsselmenge verschlüsselt, wie kann diese wieder entschlüsselt werden ?
16. Welche Probleme (in welchem Anwendungsszenario) der klassischen public-key Krpytographie löst multiple key public key Kryptographie ?
17. Was ist das Grundprinzip von XOR-basiertem Secret Splitting wenn man eine nachricht in N Teile splitten will ? Mit wievielen Teilen kann man die Nachricht wieder rekonstruieren ?

Fragen zum Skriptum - Abschnitt 1.3.3.11 - 2.1.2

18 ** Wie funktioniert Shamir's Secret Sharing (mit numerischem Beispiel) ? **

19 Aus welchem Jahr stammt DES ? Ist dieses hohe Alter ein grundsätzliches Problem für kryptographische Algorithmen ? Begründen sie ihre Antwort !

20 Warum wurde / wird die Involvierung des NBS bei der Entwicklung von DES aus IBM Lucifer als Problem gesehen ?

21 Wie heisst der SOTA Nachfolgealgorithmus von DES ?

22 Welche Klasse von Verschlüsselungsalgorithmus ist DES und wie sind die wesentlichen Parameter ?

23 Was sind Confusion und Diffusion und mit welchen fundamentalen kryptographischen Grundalgorithmen werden sie erreicht ?

24 Warum erfüllt das DES Design das Kerckhoff'sche Prinzip ?