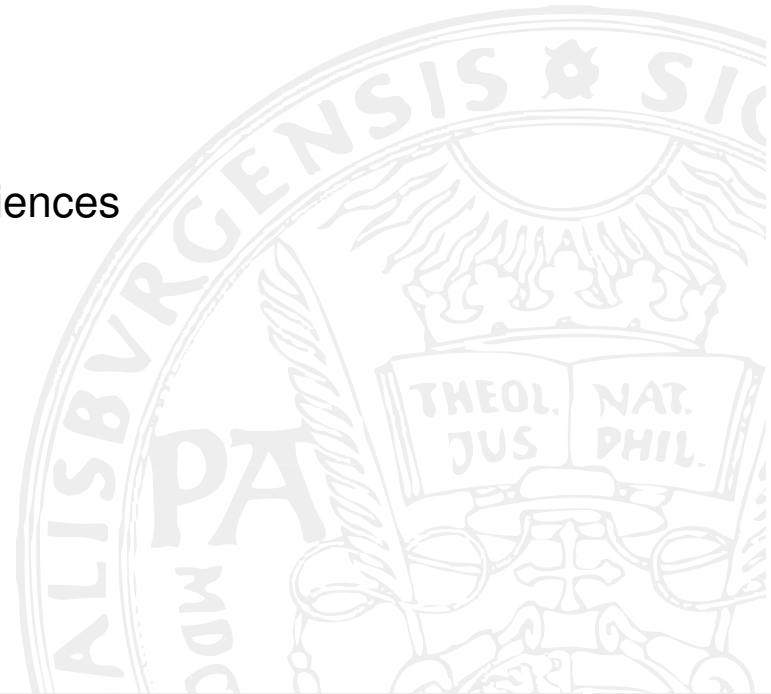
Einführung Kryptographie und IT-Sicherheit

Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

Mai 11th, 2020



Fragen zum Skriptum - Abschnitt 2.2.1 - 2.2.2

1. Wenn n eine Primzahl ist, warum ist dann $\phi(n) = n - 1$?
2. *** Ist $n = pq$ mit p, q Primzahlen, warum ist dann $\phi(n) = (p-1)(q-1)$? ***
3. Warum ist $a^{\phi(n)-1} \mod (n)$ invers zu a ?
4. *** Bestimmen sie alle Primitivwurzeln Modulo 11 (verwenden sie ein anderes – effizienteres – Kriterium als die in der VO verwendete Definition) und zeigen sie anhand einer Gefundenen dass diese auch das Definitionskriterium erfüllt. ***
5. Was ist ein Galois Feld ? Was sind die beiden grundlegend unterschedlichen Typen ?
6. Beschreiben sie das Setup von RSA (also welche Parameter müssen wie gewählt werden ?) !
7. *** Beweisen sie die Korrektheit der Formeln für die RSA Ver- und Entschlüsselung für den Fall $(m_i, n) = 1$. ***

Fragen zum Skriptum - Abschnitt 2.2.2 - 2.2.2.3

8. *** Beweisen sie die Korrektheit der Formeln für die RSA Ver- und Entschlüsselung für den Fall $(m_i, n) \neq 1$. ***
9. Was hat $(m_i, n) \neq 1$ allerdings für negative Konsequenzen ? Wie wahrscheinlich ist das ? Abhilfe ?
10. Was ist schneller ? RSA oder triple-DES (also dreifache DES Ausführung) ?
11. *** Gegeben sind als public key $n = 21$ und $e = 5$. Sie fangen einen Ciphertext $c = 2$ ab. Ermitteln Sie durch eine Faktorisierungs-Attacke den dazugehörigen Plaintext und erklären Sie die Rolle der Faktorisierung bei Ihrer Attacke.***
12. Beschreiben sie die Durchführung des Angriffs nach Szene 1.
13. Szene 1 – welche Vorraussetzung ist eventuell unrealistisch für die Durchführung des Angriffs ?
14. Beschreiben sie die Durchführung des Angriffs nach Szene 2.

Montag 11 Mai, 13:15

Fragen zum Skriptum - Abschnitt 2.2.2.3 - 2.2.2.4

15. Szene 2 – welche Vorraussetzung ist eventuell unrealistisch für die Durchführung des Angriffs ?
16. Beschreiben sie die Durchführung des Angriffs nach Szene 3.
17. Szene 3 – welche Vorraussetzung ist eventuell unrealistisch für die Durchführung des Angriffs ?
18. *** Diskutieren sie die Möglichkeiten in Szene 1 - 3, die zu unterschreibenden Daten so “hinzubiegen” dass sie für die unterschriebenden Parteien nicht zufällig, sondern inhaltlich o.k. wären. ***
19. *** Diskutieren sie für die drei Szenen detailliert, inwieweit die Anwendung einer One-Way Hash Funktion bei der Unterschriftsleistung die Sicherheit verbessert. ***
20. Erklären die die Common Modulus Attacke.
21. Wie kann dieser Angriff vermieden werden ?

Montag 11 Mai, 13:15

Fragen zum Skriptum - Abschnitt 2.2.2.5 - 3.1.1

22. Was ist die Low Encryption Exponent Attacke ? Wie kann sie vermieden werden ?
23. *** Warum ist “Textbook-RSA” wie bisher diskutiert unsicher ? Inwiefern löst “padded-RSA” diese Problematik ? ***
24. Erklären sie die dargestellte Attacke gegen Verschlüsselung und Signierung. Abhilfe ?
25. Erklären sie die “Meet in the middle Attacke”. Inwieweit verringert sie die Angriffskomplexität ?
26. Erklären sie die Oorschot-Wiener Attacke gegen DES triple-Encryption mit 2 Keys.
27. Bestimmen sie die Angriffskomplexität gegen DES triple-Encryption mit 3 Keys.
28. Wie sehen triple-Encryption CBC Varianten aus ? Welche Variante ist am sichersten ?