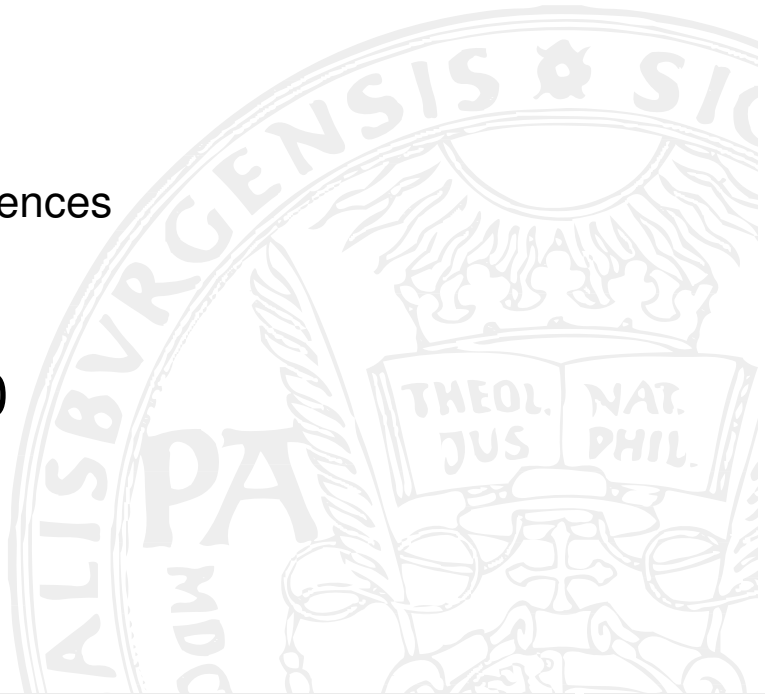
Einführung Kryptographie und IT-Sicherheit

Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

March 30th, 2020



Montag 30 März, 13:15

Fragen zum Skriptum - Abschnitt 1.3.1.4

1. Warum ist Verschlüsselung mit XOR ein symmetrisches Verfahren mit identischemVer- und Entschlüsselungskey ?
2. Erklären sie wie das “counting coincidences” funktioniert unter Ausnutzung des Index of coincidence (was ist letzteres ?).
3. Warum verändern monoalphabetische Substitution Ciphers den IoC nicht ?
4. Warum fallen bei einem Shift um ein Vielfaches der Keylänge (und dem XOR der Ciphertexte) die Keys weg ?
5. Welche Alternativen gibts es zur Bestimmung der Keylength in short-key XOR zur Counting coincidences Methode ?
6. Welche Entschlüsselungsmethode folgt direkt aus der Erkenntnis, dass short-key XOR ein Polyalphabetischer Substitution Cipher ist (zusammengesetzt aus mehreren monoalpahbetischen) ?
7. Was ist ein “Text Autokey Cipher” ? Zusammenhang mit short-key XOR ?

Montag 30 März, 13:15

Fragen zum Skriptum - Abschnitt 1.3.1.5 - 1.3.2.3

8. Wie kann OTP Verschlüsselung angegriffen werden wenn der gleiche Key wiederverwendet wird ?
9. Was bewirkt zusätzlich eine known-Plaintext Attacke ?
10. Welche Eigenschaft des OPT keystreams ist wesentlich für die Sicherheit ? Was bedeutet das für die Verwendung von PRNG zur Erzeugung des OTP ?
11. Welche Personen sind typische kryptographische ProtokollteilnehmerInnen und was ist deren Aufgabe ?
12. Erklären sie verschiedene Protokolltypen und deren Vor- und Nachteile.
13. Welche Attacken gibt es gegen kryptographische Protokolle und welche Rolle haben dabei die legitimen TeilnehmenrInnen ?
14. Vergleichen sie für n Nutzer die Anzahl der notwendigen Schlüssel im Fall von symmeterischer und public-key Kryptographie.

Montag 30 März, 13:15

Fragen zum Skriptum - Abschnitt 1.3.2.3 - 1.3.3

15. Betrachtend Input und Output einer One-way Funktion, was ist fixed length und was variable length ?
16. Kann man aus der Gleichheit von zwei Hash Werten zwingend ableiten dass die Pre-images gleich waren ? Begründen sie ihre Antwort !
17. Was ist eine Message Authentication Code ? Was kann die Abkürzung MAC noch bedeuten (in der Netzwerktechnologie) ?
18. Betrachtet man public-key Kryptographie im Kontext von One-way Funktionen, was ist hier das Trapdoor ?
19. Was sind Nachteile von public-key Verfahren (neben dem Vorteil des effizienten Key managements) ?
20. Was ist die Idee von hybriden Systemen (also symmtrische + public-key Verfahren) ? Welche Vorteile werden genutzt, welche Nachteile vermieden ?

Montag 30 März, 13:15

Fragen zum Skriptum - Abschnitt 1.3.3 - 1.3.3.3

21. Vergleichend analoge und digitalisierte Unterschriften, welche Eigenschaften der analogen Unterschrift können nicht ins digitale übertragen werden ? Warum ?
22. Erklären sie das Konzept der digitalen Unterschrift unter Einsatz von symmetrischer Verschlüsselung und eines Arbtitrators (einer trusted third party).
23. Erklären sie das Konzept der digitalen Unterschrift unter Einsatz von public key Methoden.
24. Warum werden bei digitalen Unterschriften Hashfunktionen eingesetzt ?
25. Welche beiden kryptographischen Grundfunktionalitäten werden beim Einsatz einer digitalen Signatur eingesetzt ?
26. Wie können public-key digitale Unterschriften mit public-key Verschlüsselung kombiniert werden ?