Applications to Cryptography

Proseminar
Gabriel Gäßler

Inhaltsverzeichnis

Abstract :

In dieser Präsentation wollen wir uns Anwendungen in der kryptographischen Welt anschauen. Zuerst stelle ich vor, was wir allgemein unter Kryptographie verstehen und was die Motivation dahinter ist.
Im Anschluss schauen wir uns die gängige Notation und Definition an und formalisieren das Ganze mit einem kleinen Beispiel aus dem ersten Jahrhundert v.Chr.

Das Hauptthema wird die asymmetrische Kryptographie sein. Hier diskutieren wir, was ein Public-Key-Verfahren ist und gängige Anwendungen von Verschlüsselungsalgorithmen.

Zum Schluss erkläre ich noch, was man unter einer Signatur versteht mit einem Ausblick auf die Anwendung.