Einige nützliche Python-Programme

Grundlegendes

Zur Vorbereitung auf die Online-Tutorien und die Klausur finden Sie hier eine Aufstellung nützlicher Python-Funktionen zur Analyse kryptographischer Zusammenhänge. Bitte stellen Sie sicher, dass die Funktionen auf Ihrem Rechner am Prüfungstag funktionieren.

Hinweis: Einige Python-Programme erfordern die Installation der Python-Bibliothek "Numpy". Numpy ist ein Akronym und steht für "Numerisches Python". Die Python-Bibliothek muss separat installiert werden. Die Installation wird empfohlen!

Bei Fragen kontaktieren Sie mich bitte!

Endlicher Zahlenkörper

Die nachfolgende Tabelle listet einige im Lehrbrief verwendete Python-Funktionen in Verbindung mit Berechnungen auf dem endlichen Zahlenkörper auf.

Funktion	Bibliotheken	Erklärung
ggt.py	–	Ermittlung des größten gemeinsamen Teilers
m_inverses.py	–	Bestimmung des multiplikativ inversen Elementes
euler_phi.py	–	Bestimmung von $\Phi(n)$

Hash-Funktionen

Die nachfolgende Tabelle listet einige im Lehrbrief verwendete Python-Funktionen in Verbindung mit der Berechnung von Hashwerten auf.

Funktion	Bibliotheken	Erklärung
hash-lib.py	hashlib	u.a. Hashing eines Passwortes
SHA-variable.py	hashlib	Eigenschaften der Hash-Funktionen
verify-hash.py	hashlib	Vergleich von Hashwerten
verify-hash-salt.py	hashlib, uuid	Hashwert eines Passwortes mit Bezug Salt

Ver- und Entschlüsselung

Die nachfolgende Tabelle listet einige im Lehrbrief verwendete Python-Funktionen für die Ver- und Entschlüsselung auf.

Funktion	Bibliotheken	Erklärung
haeufigkeitsanalyse.py	Numpy	Häufigkeitsanalyse
caesar.py	–	Caesar Ver- und Entschlüsselung
spaltentransposition.py	–	Entschlüsselung Spaltentransformation
rsa_key.py	–	RSA Schlüsselerzeugung
rsa_encrypt.py	–	RSA Verschlüsselung
rsa_decrypt.py	–	RSA Entschlüsselung
rsa_web_modi.py	–	RSA Ver- und Entschlüsselung
code_error_1.py	Numpy	Analyse (5,2) Blockcode
code_based_1.py	Numpy	Beispiel codebasierte Kryptographie

Post-Quanten Kryptographie

Die nachfolgende Tabelle listet einige im Lehrbrief verwendete Python-Funktionen für die Schlüsselerzeugung, Ver- und Entschlüsselung auf.

Funktion	Bibliotheken	Erklärung
lwe_bsp.py	Numpy	LWE (Beispiel entsprechend Skript)
lwe.py	Numpy	LWE (allgemein)