Aufgabe 10

Symmetrische Kryptografie

Kryptografische Verfahren, bei denen Sender und Empfänger denselben Schlüssel zum Ver- wie auch zum Entschlüsseln von Nachrichten verwenden, werden symmetrische Verschlüsselungsverfahren genannt.
Viele historische Verschlüsselungsverfahren (wie Caesar-Verschlüsselung oder auch „Enigma“ - welche z.B. im 2.Weltkrieg eingesetzt wurde) verwendeten symmetrische Verfahren, es gibt aber auch modernere symmetrische Verfahren wie AES (Advanced Encryption Standard) oder IDEA (International Data Encryption Algorithm).
Symmetrische Verfahren bieten im Vergleich zu asymmetrischen Verfahren unter anderem den Vorteil der schnelleren Berechenbarkeit.
Dem gegenüber steht der Nachteil des Schlüsselaustauschproblems: Beide Kommunikations-teilnehmer müssen den gemeinsamen Key (PreSharedKey) vorab über einen abhörsicheren Weg austauschen.

Aufgaben

a) Suchen Sie aus dem **Herdt-Buch „Netzwerke-Sicherheit“ - Kapitel 10** Antworten für folgende Fragen:

- Was bedeuten die Begriffe Kryptografie und Kryptoanalyse?
- Von wem stammt das Prinzip, dass die Sicherheit einer Verschlüsselung ausschließlich vom Schlüssel abhängig sein soll und nicht durch Geheimhaltung des Algorithmus („Security through obscurity“)?

- Worin liegt der Schlüssel bei der Stabchiffre (Skytale)?
- Skytale ist eine Transpositions-Chiffre. Was bedeutet Transposition?
- Bei der Caesar- bzw. ROT-Verschlüsselung handelt es sich um eine Substitutionschiffre. Was bedeutet Substitution?
- Wie viele sinnvolle Schlüssel gibt es bei der Caesar- bzw. ROT-Verschlüsselung?
- Welche Rolle spielt der Buchstabe „E“ bei der Kryptoanalyse eines ROT-verschlüsselten Textes?
- Was unterscheidet die Vigenère-Chiffre von einer ROT-Chiffre?

- Worin unterscheiden sich Block- von Stromchiffren?
- Aus wie vielen Bits bestehen die Schlüssel bei DES (Data Encryption Standard), bei 3DES (Triple DES) bzw. bei AES (Advanced Encryption Standard) ?

- Was unterscheidet ECB (Electronic Codebook) und CBC (Cipher Block Chaining)?

b) Übungsbeispiele:

- Sie haben einen **CAESAR/ROT**-verschlüsselten Ciphertext:
  FKGUGT VGZV KUV FKG MQTTGMVG NQGUWPI

  Welche Möglichkeiten haben Sie, den Plaintext (unverschlüsselte Nachricht) zu finden?
  - Wie viele Varianten gibt es für Brute-Force-Angriff?
  - Welcher Buchstabe kommt im verschlüsselten Text am häufigsten vor?
  - Lässt dies Rückschlüsse auf den verwendeten Key zu?

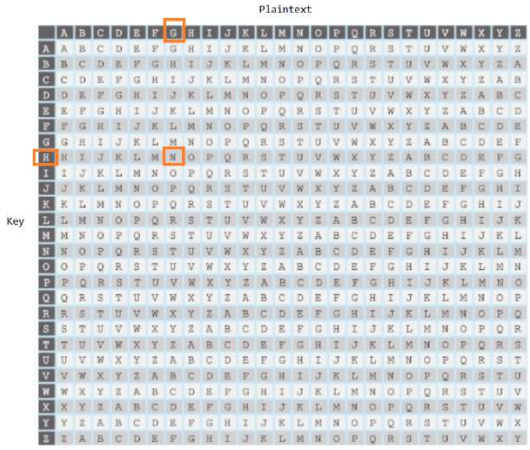
  Wie lautet die Lösung?

  Testen Sie das Java-Programm „Caesar.java“ – (Sourcecode auf Moodle)
  Testen Sie die CAESAR-Entschlüsselung auf https://cryptii.com/

- Der Plaintext „GEHEIM“ soll **Vigenère** verschlüsselt werden. Der Key ist „HTL“.
  Wie lautet der verschlüsselte Text?

Plaintext	G	E	H	E	I	M
Key	H	T	L	H	T	L
Ciphertext	N	X	S	L	B	X

  Anmerkung: Da der Schlüssel kürzer ist, als der Plaintext, wird er mehrmals hintereinander geschrieben



- Entschlüsseln Sie den **Vigenère** verschlüsselten Text (Key ist „HTL“):

Ciphertext	R	H	C	Y	X	V	A
Key	H	T	L	H	T	L	H
Ciphertext	K	O	R	R	E	K	T

  Vergleichen Sie Ihre Ver-und Entschlüsselung mit https://cryptii.com/