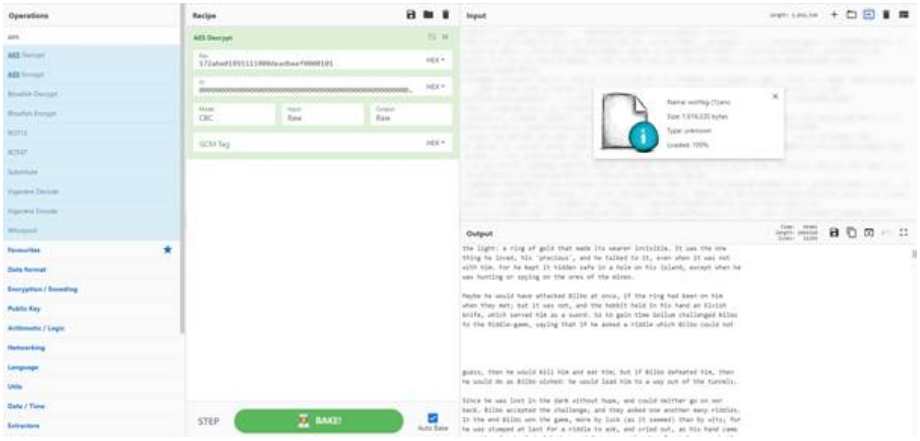
Angewandte Kryptographie

David Zeilinger

Aufgabe 1 - Ransomware

Rekonstruiere den inhalt von wichtig.enc

Letzten 256 bytes aus wichtig kopieren und mit dem priv-key decrypten => 172abe01891111000deadbeef000011



Cyberchef

Aufgabe 2 - Tink

Wir sollen Mittels Tink einen Text Ver- und wieder Entschlüsseln.

Code

```
import com.google.crypto.tink.*;
import com.google.crypto.tink.aead.AeadFactory;
import com.google.crypto.tink.aead.AeadKeyTemplates;

import java.security.GeneralSecurityException;

import com.google.crypto.tink.KeysetHandle;
import com.google.crypto.tink.config.TinkConfig;



public class Gen {

    public static void main(String[] args) throws
GeneralSecurityException {
```

```
        TinkConfig.register();
        try {

            String plaintext="I'm blue.";

            // Generate the key material...
            KeysetHandle keysetHandle =
KeysetHandle.generateNew(AeadKeyTemplates.AES128_GCM);
            Aead aead =
AeadFactory.getPrimitive(keysetHandle);



            String aad="bla";
            System.out.println("Text: "+plaintext);

            //encrypt obj
            byte[] ciphertext =
aead.encrypt(plaintext.getBytes(), aad.getBytes());

            String enc = new String(ciphertext);
            System.out.println("Cipher: "+enc);

            //decrypt obj
            byte[] decrypted = aead.decrypt(ciphertext,
aad.getBytes());

            String dec = new String(decrypted);
            System.out.println("Text: "+dec);

        } catch (GeneralSecurityException e) {
            System.out.println(e);
            System.exit(1);
        }
    }
}
```

Ergebnis

Text: I'm blue.
Cipher: □□®?Pü®Xµ)x…□øÛ,n½›_□æ
Text: I'm blue.

AEAD

AEAD bezieht sich einfach auf die Betriebsmodi für die Cypher. Sie sind eine Gruppe an Betriebsmodi, die nicht nur Das Ergebnis besser Verschlüsseln, sondern auch die Authentität der daten sicherstellen.

GCM

GCM ist ein weiterer Betriebsmodi, wie jene, die wir schon in unserer Ausarbeitung erfasst haben.

Bei ihm ein pro Block eindeutiger Zähler verwendet, die Blockgröße der Blockchiffre ist auf 128 Bit festgelegt.