Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

1. Assignment: From paleo-cryptography to AES

(Hand in solutions on Thursday, November 15th during the lecture)

Exercise 1.1 (Le chiffre indéchiffrable). (4 points)

Directly inspired from the Caesar cipher, the Vigenère cipher[1] uses successively different keys for each letter of the plaintext.

The key of the Vigenère cipher is then a word of the alphabet. The first letter of the plaintext is encoded with the Caesar cipher using the first letter of the key as the key, the second letter of the plaintext encoded using the second letter of the key, and so on, the key being repeated several times to match the length of the plaintext if necessary.

For instance, using the key "FORTYTWO", the plaintext "THE HITCHHIKER'S GUIDE TO THE GALAXY" would be encrypted as follows:

Plaintext	THE HITCHHIKER'S GUIDE TO THE GALAXY
Key	FOR TYTWOFORTYTWOFOR TY TWO FORTYT
Ciphertext	YVV AGMYVMWBXP'L CINRV MM MDS LOCTVR

(i) Using the same key, decode the ciphertext "ICE'M NTJWH". 1

We now suppose that we are given the ciphertext of an English message, which we know is much longer than the key that was used, even though we don't know the actual length of this key. Let's try to find out how to break the cipher and retrieve the plaintext.

(ii) The first thing to do is to find the key length. Can you think of a way to do that efficiently? 1

(iii) Once the length of the key is known, how can you retrieve the actual key and the plaintext? 1

(iv) What can you say about the security of the Vigenère cipher? 1

[1] <historical digression>Named after Blaise de Vigenère, but actually first described 1553 by Giovan Battista Bellaso. Vigenère also developped a similar (although stronger) cipher in 1586, but Bellaso's work was attributed to him, though he had nothing to do with it[2].</historical digression>

[2] Thank you, Wikipedia!

Exercise 1.2 (AES amputated). (9 points)

As we have already seen during the lectures, AES is an extremely simple cipher, its description is very short. But still, can we make it even simpler, by hacking out superfluous bits without impacting on its strength?

Considering the four steps (`SubBytes`, `ShiftRows`, `MixColumns` and `AddRoundKey`) performed in each round, we want to see whether those steps are essential or not to the security of the cipher.

[2] (i) For instance, what would happen to AES should one remove the `SubBytes` step in each round?

[2] (ii) What if one were to remove the `ShiftRows` step?

[2] (iii) What about the `MixColumns` step?

[2] (iv) And the `AddRoundKey` step?

[1] (v) Conclude.