Wednesday, May 13th, 2015 Introduction to Cryptology and Coding Exam M1 MOSIG

Prof. J-G. Dumas 3 HOURS : **Only written notes and course documents allowed.**

1 Frequency analysis

Consider ZWUM PIA AMDMV PQTTA, a text of 18 letters. Suppose that this is a secret message obtained via a Caesar's cipher.

1. Give four candidates for the cipher letter corresponding to the encryption of an E in the original message (written in English).
2. For your first hypothesis, give the possible decryption of these four candidates.
3. Do the same for the three other hypothesis.
4. Knowing that ETAOIN SHRDLU is the approximate order of frequency of the 12 most commonly used letters in the English language, conclude on the most probable hypothesis.
5. Decipher the message

2 Modular arithmetics

1. Compute $5^{2015} \mod 51$.
2. Compute $100 \mod 51$.
3. Compute $5^{16} \mod 51$.
4. Show that 5 is a Miller-Rabin witness of compositeness for 51.

3 Insecure channel protocol

In a certain protocol, Alice will at a given time send one of 16 possible commands to Bob. Based on this command, Bob will perform some action (observable by anyone, and Eve in particular) the day after the protocol completes. This is repeated everyday, so that the action Bob performs on Monday is determined by the command sent by Alice on Sunday. The channel used for the protocol is insecure, so to keep the command secret it is encrypted using a function f and a key k shared by Alice and Bob. Four bits are used to represent the command, and the remainder of the bits in the block m are set to 0. Then Alice sends $c = f(k, m)$ over the insecure channel.

Eve wants to know which command was sent by Alice before Bob actually performs the specified action.

1. Explain how Eve is able to determine this after listening to the protocol executions for a few weeks.
2. Can you suggest a simple modification to the protocol that will protect against the passive listener Eve.

4 Hybrid cryptology

A group of n people want to use a cryptographic system to exchange confidential information items on a two-by-two basis. The information items to be exchanged between two members of the group must not be readable by another member.

1. What is the minimum number of symmetric keys which are required?
2. What is the minimum number of asymmetric keys which are required?
3. The group finally uses a hybrid system for encryption. Describe the elements of such a hybrid systems and the reasons for such a choice.

5 LFSR mod 5

Find the LFSR that generates the following flow modulo 5:

$$0, 3, 0, 1, 3, 2, 2, 2, 1, 1, 4, 3, 4, 0, 1, 4, 2, 4, 3, 0, 0, 3, 0, 1, 3, 2, 2, 2, 1, 1, 4, 3, 4, 0, 1, 4, 2, 4, 3, 0, 0, 3, 0$$

6 Attack on RSA

Note: Questions in this exercise are mostly independent.

Alice has a RSA pair of keys: (e_A, n_A) is her public key and (d_A, n_A) her private key. We now suppose that Alice's public key is $(e_A = 317, n_A = 667)$. We will try to break Alice's key.

1. Find the smallest integer x such that $n_A + x^2 = y^2$, where y is a positive integer.
2. Deduce from this relation that 23 is a factor of n_A.
3. Recall the relation that must satisfy e_A, d_A and n_A.
4. What algorithm can you use to compute d_A from e_A and n_A? (name it and write down the algorithm)
5. Apply it to compute the actual value of d_A.

7 AES 128 bits

7.1 Complexity of AES

Suppose it is possible to find, for 100€, a processor that can exhaustively try 1 billion (10^9) AES-128 keys per second. Suppose also that an organization is eager to spend 2000 billions of euros (this is the order of magnitude of the budget of France) to an exhaustive search of a single AES-128 key. Ignoring additional costs (such as energy, support, etc.) how long would it take?

7.2 ShiftRows

Apply ShiftRows on the message:

```
1D 32 7C D5 13 42 BB 9A 1F 73 6E 74 80 66 C0 39
```

7.3 SubBytes

With the classical parameters of the AES ($P_8 = X^8 + X^4 + X^3 + X + 1$; $SubBytes$ matrix being the circulant 8×8 of the row 1000 1111; and initialization vector being $1 + X + X^5 + X^6$, bits low to high from up to bottom), Prove that $SubBytes([F6]) = [42]$.

7.4 MixColumn

With the classical parameters of the AES (the same as in preceding question and MixColumn matrix being the circulant of the first row $[03], [01], [01], [02]$, or equivalently the MixColumn multiplication being done by $G = [03]Y^3 + Y^2 + Y + [02]$, modulo $Y^4 + 1$), evaluate the column mixing of: $\begin{bmatrix} [00] \\ [01] \\ [00] \\ [AB] \end{bmatrix}$.

7.5 AES without SubBytes

We here suppose that the SubBytes transform are taken out of the AES algorithm. Let x be a 128 bits word and $y = E(x)$ its cipher via this modified AES. We now suppose that an adversary intercepted the cipher Y and knows the associated clear text x.

1. What is obtained during the first round, after `AddRoundKey` and `ShiftRow` for an abstract round key $K0 = [K0_i]$?
2. Then what is obtained after the first `MixColumn`?
3. Suppose then that y and its associated cleartext x are known, and suppose that there is a single round, show that it is easy to recover $K0$.
4. What happens after several rounds of this kind?