INGI2347 : Exercises
Lab 2 [*]

Xavier Carpent

March 2, 2015

Solution 1: Exhaustive Search for Symmetric Keys

Knowing that the “DES-Cracker ” takes on an average 4.5 days (i.e., 388.800 seconds) to find a 56-bit DES key, cracking a 40-bit key would require on an average

$$\frac{2^{40}}{2^{56}} \times 388.800 \approx 5.9 \text{ s}$$

while a 112-bit key would require

$$\frac{2^{112}}{2^{56}} \times 388.800 \approx 2.8 \times 10^{22} \text{ s}$$

and a 256-bit key

$$\frac{2^{256}}{2^{56}} \times 388.800 \approx 6.3 \times 10^{65} \text{ s}$$

The last two numbers represent durations of 68290 times and of 1.5×10^{48} times the universe’s age (estimated at 13 billion years) respectively.
It is interesting to note that it takes on average 4.5 days of calculation to find a 56 bits DES key with the DES-Cracker, which means that in the worst case, this machine would need 9 days of calculation to find a 56 bits DES key, i.e., to test *all* the 2^{56} possible keys.

Solution 2: Symmetric and Asymmetric Encryption

1. Since the information exchanged between two group members must not be readable by any other member, we require one symmetric key per pair of potential correspondents, i.e., a total number of $n(n-1)/2$ keys.

2. Here are a few well known symmetric encryption algorithms: AES, Triple-DES, IDEA.

3. Each group member must have a pair (public key, private key); thus we will need at least n pairs of keys in the group.

4. Bob must use his own private key for signing and Alice’s public key for encryption.

5. Here are a few well known asymmetric encryption algorithms: RSA, ElGamal.

6. Symmetric algorithms are much faster than asymmetric algorithms. Unfortunately, on the one hand the exchange of symmetric keys is more delicate (we need a confidential *and* authenticated

[*] A part of these exercises comes from the book “Computer System Security”. The reproduction and distribution of these exercises or a part of them are thus forbidden.

channel) and on the other hand, symmetric cryptography does not answer all the criteria that one expects from a signature schema (we cannot distinguish if it is the sender or the recipient who signed: repudiation problem). By using a hybrid system (it is the solution chosen by PGP or SSL, for example, that encrypt the symmetric key with an asymmetric key), we benefit from the advantages of asymmetrical cryptography and simultaneously preserve the efficiency of symmetric cryptography.

Solution 3: Loss of a Private Key

1. Alain is still able to send encrypted mails since for that, he uses the recipient's public key. As long as he does not revoke the public key corresponding to his lost key, he will still certainly receive encrypted mails, but he will not be able to decrypt them.

2. He can no more sign electronic mails he sends since for that, he uses his own private key. However, he will still be able verify the signature of the mails he receives, using the sender's public key.

3. Before anything else, it is very important to revoke the lost key. Then, a new pair must be obtained (public key, private key).

Solution 4: Kerckhoffs' Principles

The principle proposed in this exercise is one amongst those established by Auguste Kerckhoffs in January 1883, in *Journal des sciences militaires*, vol. IX, pp. 5–38. This fundamental principle stipulates that the security of a cryptographic algorithm must not rely on its secrecy, but on the fact that is "modulated" by a *key*. The fact that the algorithm is public should not compromise its security. Indeed, although keys can be frequently changed, it is impossible to keep a cryptographic algorithm secret: past experiences have shown that such algorithms always ends up becoming public, one way or the other.

Solution 5: Symmetric Encryption Modes

1. In the ECB mode, two identical data blocks will always be encrypted in an identical way. For example, by encrypting an ASCII file whose contents are

```
Monthly salaries of Startup Ltd.
------------------------------------------------
Alice Terrique                 14567,89 EUR
Alain Terrieur                  2000,00 EUR
Alex Terrieur                   2000,00 EUR
```

in ECB mode with AES, Alain Terrieur could easily realize that he earns the same salary as his brother Alex, since the encrypted blocks corresponding to the salaries will be equal. Moreover, the two brothers can also find out that Alice Terrique earns a salary different from theirs. One could also imagine that Alex or Alain replace the encrypted block of his salary by that corresponding to Alice's, so long as the file's integrity is not verified.

2. If two encrypted blocks Y_i and Y_j are equal and we have the preceding blocks Y_{i-1} and Y_{j-1}, we can deduce that the data entering the encryption algorithm are identical (otherwise, the latter would not be able to decipher this block): $X_i \oplus Y_{i-1} = X_j \oplus Y_{j-1}$. If one denotes this input as S,

and we combine Y_{i-1} and Y_{j-1} using $\oplus$, we obtain $Y_{i-1} \oplus Y_{j-1} = X_i \oplus S \oplus X_j \oplus S = X_i \oplus X_j$, since $S \oplus S$ is always equal to 0. A collision thus reveals the XOR of two data blocks of the clear text, which allows recovering X_i or X_j in certain cases.

3. The birthday paradox indicates that after having observed 2^{32} data blocks (which corresponds to 32 GB of encrypted data in the case of Triple-DES), the probability of observing a collision is approximately equal to 40%. This explains why the successor of DES, the AES algorithm, has a block size of 128 bits: in this case, it would be necessary to observe 2^{64} blocks of 128 bits to obtain the same success probability, which is unrealistic with the current technology.