**Home Assignment no 3 – Modes of Operation**

**Requirements** (points will be taken if the requirements are not fulfilled):

1. The assignment is due 20/05, time 23:55. To be submitted in singles or pairs only.
2. To submit: the whole project with the detailed PDF describing each task separately, the language chosen, the padding chosen, the description of encryption and decryption. You are to add the signed document of originality (found in Moodle). To be submitted as a ZIP file.
3. The ZIP file must be named with the full names of both partners (or a single partner).
4. There must be a strict separation between the tasks (functions, classes, etc. depending on what is relevant to the language chosen).
5. Must be submitted in Moodle only. In any case it will not be accepted by other means.

**For all the tasks:** you are to encrypt the given text with the **key= nonsense** and the **IV = mySecret**; and decrypt the cipher. For both processes use the DES algorithm that you already implemented.

Important: it is forbidden to use any open source, all the functions must be implemented by yourselves.

**Padding**: you are to decide by themselves what you add to the last block if it contains less than 64 bit. This must be stated in your DPF file!!!!!

The modes of operation are separated into 4 tasks:

**Task 1.**

Electronic Code Book (ECB). Reminder: no **IV** is needed.

**Task 2.**

Cipher Block Chaining (CBC).

**Task 3.**

Cipher FeedBack Mode (CFB).

**Task 4.**

Output FeedBack Mode (OFB). You are to perform precomputing before encrypting and decrypting.

**Task 5.** (Bonus – 10 pts.)

Counter Mode (CTR) – to be learned and implemented by yourselves.

**The plaintext to be encrypted in all the tasks is:**

The Concise Oxford English Dictionary defines cryptography as “the art of writing or solving codes.” This is historically accurate, but does not capture the current breadth of the field or its present-day scientific foundations. The definition focuses solely on the codes that have been used for centuries to en-able secret communication. But cryptography nowadays encompasses much more than this: it deals with mechanisms for ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, electronic auctions and elections, digital cash, and more. Without attempting to provide a complete characterization, we would say that modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks. The dictionary definition also refers to cryptography as an art. Until late in the 20th century cryptography was, indeed, largely an art. Constructing good codes, or breaking existing ones, relied on creativity and a developed sense of how codes work. There was little theory to rely on and, for a long time, no working definition of what constitutes a good code. Beginning in the 1970s and 1980s, this picture of cryptography radically changed. A rich theory began to emerge, enabling the rigorous study of cryptography as a science and a mathematical discipline. This perspective has, in turn, influenced how researchers think about the broader field of computer security. Another very important difference between classical cryptography (say, before the 1980s) and modern cryptography relates to its adoption. Historically, the major consumers of cryptography were military organizations and governments. Today, cryptography is everywhere! If you have ever authenticated yourself by typing a password, purchased something by credit card over the Internet, or downloaded a verified update for your operating system, you have undoubtedly used cryptography. And, more and more, programmers with relatively little experience are being asked to “secure” the applications they write by incorporating cryptographic mechanisms.

In short, cryptography has gone from a heuristic set of tools concerned with ensuring secret communication for the military to a science that helps secure systems for ordinary people all across the globe. This also means that cryptography has become a more central topic within computer science.

**Good luck,**

**The questions can be asked by mail: alonhkoz@ac.sce.ac.il**