**Name: محمود زكريا حسن خيري عبدالحميد خيري**

**B.N: 843**

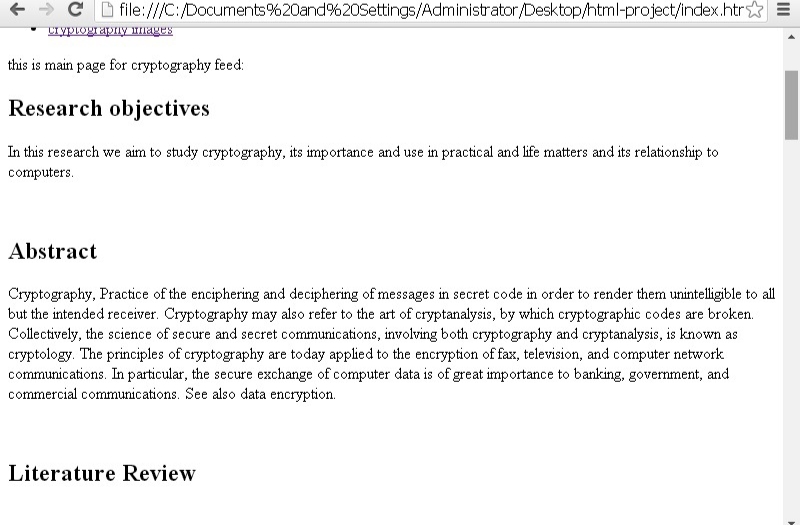
**Date: 28/may/2020**

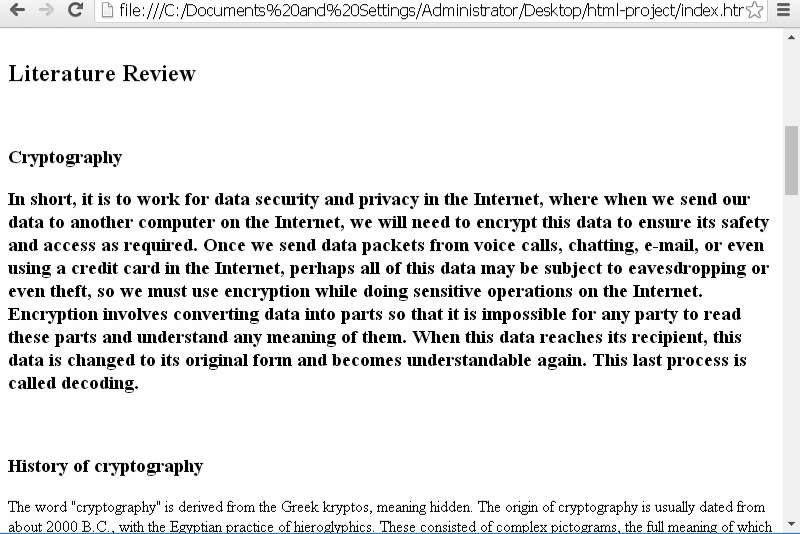
**Topic:** Cryptography

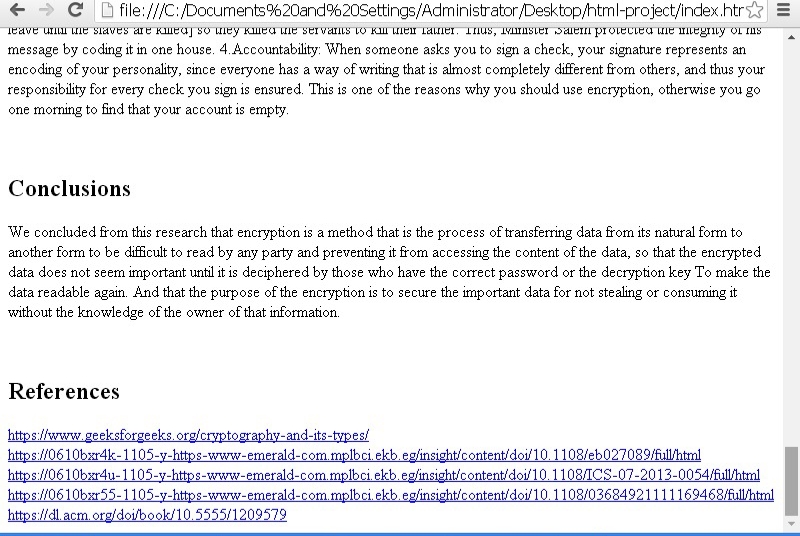
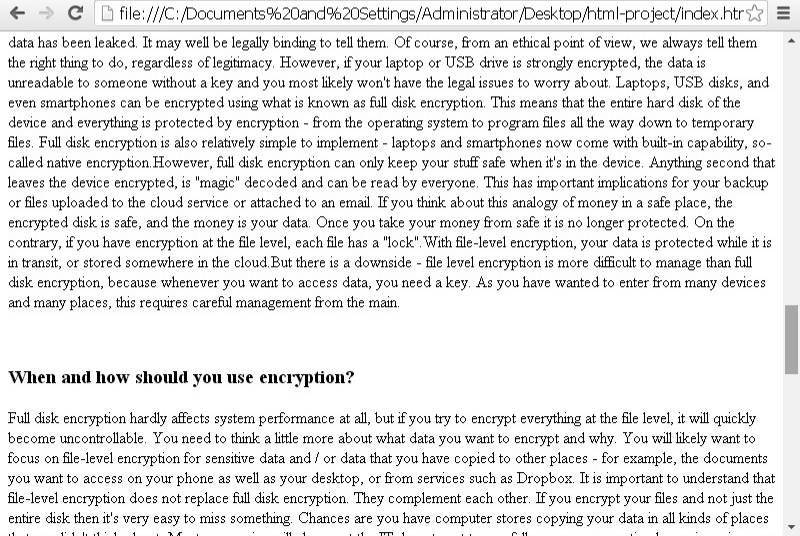
**GitHub link:** <https://github.com/MahmoudZakaria74/ece001>

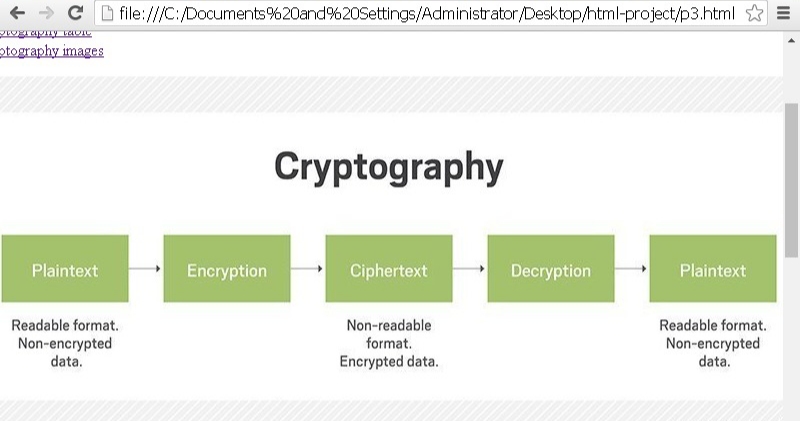
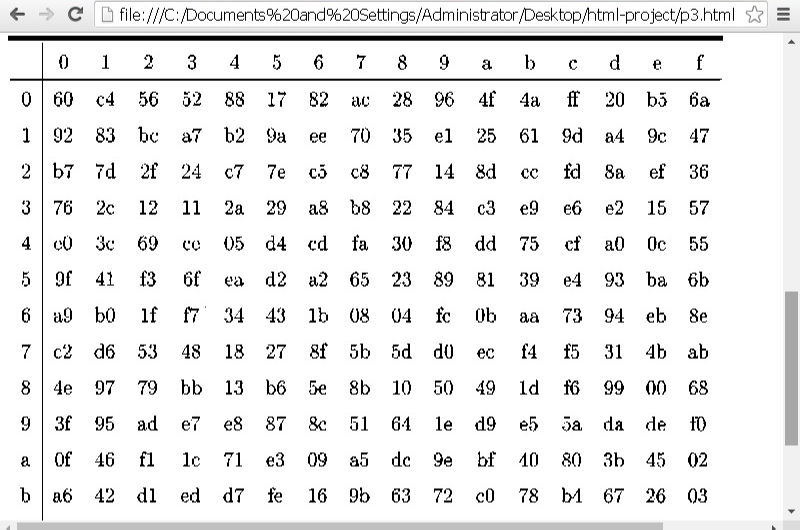
**GitHub Page:** [**https://mahmoudzakaria74.github.io/ece001**](https://mahmoudzakaria74.github.io/ece001)

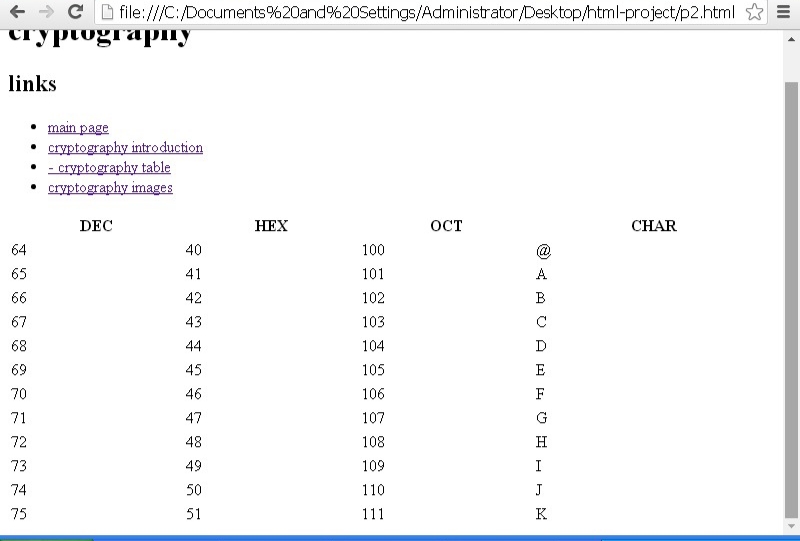
**Application brief: In the spirit of algebraic abstraction, this paper advocates the definition and use of higher levels of abstraction in cryptography (and beyond). If contrasted with the standard bottom-up approach to defining models of computation, algorithms, complexity, efficiency, and then security of cryptographic schemes, our approach is top-down and axiomatic, where lower abstraction levels inherit the definitions and theorems (e.g. a composition theorem) from the higher level, but the definition or concretization of low levels is not required for proving theorems at the higher levels. The goal is to strive for simpler definitions, higher generality of results, simpler proofs, improved elegance, possibly better didactic suitability, and to derive new insights from the abstract viewpoint. In particular, we propose a general framework for defining and proving that a system satisfying an (abstract or ideal) specification is constructed from some systems satisfying certain (concrete or real) specifications. This puts the well-known “ideal-world real-world” paradigm on a new theoretical foundation, applicable in various cryptographic settings. Existing frameworks for proving compostable security can be explained as special cases of our framework, thereby allowing to distinguish between relevant and less relevant aspects of the underlying technical definitions and to prove a single common composition theorem. Some properties of our framework are as follows. It is independent of particular models of computation, communication**

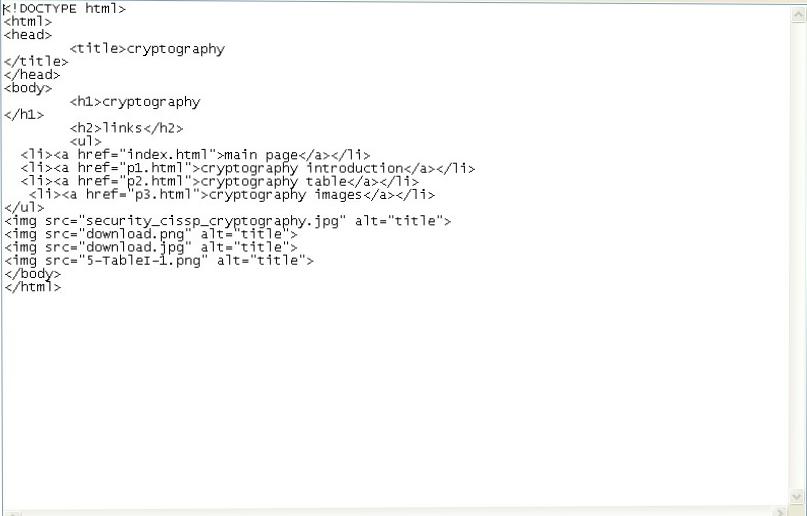
**Screeshots :**

****

****





Source code:

