Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Κρυπτογραφία

2ο Set Ασκήσεων

Διδάσκουσα: Ελισάβετ Κωνσταντίνου
Απρίλιος 2018

Αυλακιώτης Χρήστος
321/2012015

Λεπτομέριες σχετικά με την υλοποίηση:
Για την υλοποίηση των κρυπτογαφικών αλγορίθμων βάσιστηκα κυρίως στο βιβλίο "*A handbook of applied cryptography*" και στον οδηγό της βιβλιοθήκης GMP "*GNU MP Edition 6.0.0*" αλλά και σε μελέτη που έκανα στο διαδίκτυο. Προσπάθησα να μην αποκλείσω καθόλου απο τις διαδικασίες που περιγράφονται στο βιβλίο χρησιμοποιώντας τις κατάλληλες συναρτήσεις της βιβλιοθήκης GMP, και να εμφανίζω αναλυτικά μηνύματα για το τι γίνεται σε κάθε βήμα. Οι κώδικες είναι γραμμένοι σε C++03 και περιέχονται στα συννημένα της παράδοσης.