Final revision paper in cryptography:

Edited at 9am 17.1.2017.

Hash functions:

1. Calculate the hash function for your student number.

http://www.fileformat.info/tool/hash.htm

DS, MAC, KEA and DC:

2. Make digital signature (DS), Message Authentication Code (MAC), Key Exchange Authentication (KEA) and digital certificate (DC).

https://en.wikipedia.org/wiki/Digital\_signature

https://en.wikipedia.org/wiki/Message\_authentication\_code

https://en.wikipedia.org/wiki/Password-authenticated\_key\_agreement

https://en.wikipedia.org/wiki/Public\_key\_certificate

3. Create Cryptographic Algorithm (CA) and Data encryption Standard (DES).

4. Perform the imaginary money transfer using DS, DC, KEA and MAC.

Key management:

5. Manage, store and destroy key.

https://en.wikipedia.org/wiki/Key\_management

Steganography and watermarking:

6. Perform steganography and digital watermarking.

https://en.wikipedia.org/wiki/Steganography

https://en.wikipedia.org/wiki/Digital\_watermarking

Zimmermann:

7. Solve Zimmermann Polygonal Areas problem.

Based on the results, assess the probability of forging DS, MAC, KEA and DC.

http://azspcs.com/Contest/PolygonalAreas

Submit as many different areas solutions as possible in the form (1,2), (2,6), (3,4), (4,5), (6,3), (5,1) going clockwise or anti-clockwise along the border of the polygon for 11, 17, 23, 29, 37, 47, 59, 71, 83, 97, 113, 131, 149, 167, 191, 223, 257, 293, 331, 373, 419, 467, 521. For each problem we need maximum and minimum areas polygons. Do it only if you like it.

http://discrete4math.weebly.com/uploads/2/5/3/9/25393482/11polygonal11areas11zimmermann11.txt

Project:

8. Improve your project.

Deadline: before the final exam.