VE475
Introduction to Cryptography

Project 1 (04/07/2017)

Manuel — UM-JI (Summer 2017)

Goals of this project

- Improve research efficiency
- Develop teamwork and collaboration skills
- Organise and write clear documents
- Improve understanding by confronting acquired knowledge to new information

Cryptography being a vast field of study not all its subtopics can be properly considered in class. Therefore the goal of this project is to perform some personal study in order to acquire this extra knowledge while also improving major skills such as writing, collaboration, and public presentation.

As a team, discuss which subjects to investigate. In the case where everybody agrees on a topic not listed below please inform us of your choice.

This projects splits into two parts: (i) writing a report and (ii) presenting the result of your work to all the students. In particular the project report is to be submitted before the deadline and should provide a thorough presentation of the subfield of study. The presentation in front of all the students will be held at a later time and should provide a high level introduction on the chosen topic.

Any source of information can be used (internet, textbooks, research articles. . .). However, in any case, **do not recopy the materials** and always cite all your sources.

When reading new information, understand it, process it, consider how it relates to what you already know, and how you can reach conclusions beyond the ones offered in your source.

Available topics:

1. Public Key Infrastructure
2. The Random Oracle Model
3. Shannon's Theory and Cryptography
4. Error Correcting Codes and Cryptography
5. Steganography and Cryptography
6. Lattice-based Cryptography*
7. Multivariate Cryptography*
8. Message Authentication Code

*Those slightly more advanced projects will benefit from a softer grading policy.

Groups

Hu Xuefeng 胡雪峰 and Pan Shengjie 潘圣杰
Feng Yu 丰羽 and Song Jieming 宋杰铭

Han Zhuoran 韩卓然 and Mou Yipeng 牟一鹏
Wenyang 文仰 and Wu Jiaxi 吴嘉熙

Zhai Yifan 翟逸凡 and Zhang Yongyin 张永银
Tang Shenghao 汤晟皓 and Wang Zilu 王子路

Hu Qiaoyu 胡乔予 and Wei Chen 卫晨
Liu Qiyang 刘齐阳 and Sun Siqi 孙思齐

Cai Zhibo 蔡志波 and Chen yudong 陈煜东
Wang Zhiyuan 王智远 and Wei Chuxi 魏楚希

Hong Jingzhou 洪劲舟 and Huang Jingwen 黄静文
Yin Leyi 殷乐宜 and Zhang Chi 张弛

Hao Yuxuan and Xu Kejia 徐可嘉
Geng Yajie 耿亚捷 and Zhu Wenyang 朱文扬

He Zhiyuan 何知远 and Ni Yanchao 倪彦超
Xu Haining 徐海宁 and Yu Chengyun 于承运

Diao Zhuoran 刁卓然 and Gu Ronghao 顾荣豪
Gao Jiecheng 高杰诚 and Lu Yilong 陆翼龙

Li Siying 李思颖 and Wu Xinyi 吴欣怡
Peng Junda 彭俊 and Wang Dayi 王达一

Bao Shuci 包书慈 and Wang Wenhao 汪文浩
Cui Shuoyang 崔朔杨 and Qian Xiangru 钱相如

Diao Zihuan 刁梓桓 and Yang Yunlu 杨云路
Zhenwei Yang 杨振玮 and Li Xiang 李响

Zhou You 周游 and Zhao Li 赵力
Tan Lunte 谭伦特 and Wang Jingyuan 王靖元

Wang _fu 王源夫 and Wang Jie 王捷
Wang Xiangyu 王翔宇 and Xu Zilin 徐子临

Zeng Zhi 曾挚 and Zhu Chen 朱宸
Shi Yucheng 史玉成 and Xu Rishang 徐日上

Lan Tianmu 兰天牧 and Wang Yuchen 王宇辰
Wu Yuexiao 吴越箫 and Zheng Xuan 郑璇

Feng Zhengyang 冯正扬 and Zuo Jiaqi 左嘉琦
Wang Zesen 王泽森 and Xue Leyang 薛乐阳

Duan Yijian 段益坚 and Hang Wei 杭卫
Ding Kaili 丁恺笠 and Wu Chenggang 吴承刚

Song Yue 宋越 and Zhu Wenyao 朱文耀
Lu Chengzhe 陆成哲 and Zhang Jian 张简

Sato Muneyuki and Wu Yuzhou 吴禹洲
Liu Xu 刘旭 and Zhang Kai 张开

Qian Shengyi 钱圣轶 and Song Qun 宋
Chen Zhiqing 陈志卿 and Wu Jiachen 吴佳晨

Li Guohao 李国豪 and Wu Yichen 吴奕辰
Silva Rui and Wu Wenyi

Vagne Lars and Zhu Yifan 朱一凡
Gu Yichen 顾宜宸 and Liu Yihao 刘逸灏