Ecole Polytechnique Fédérale de Lausanne

Course Notes in

Cryptography and Security

Olivier Cloux

Autumn 2018

Contents

1 Ancient Cryptography

1.1 Summary

Prehistory: used for confidentiality only. Enforce by different means. Nowadays, we wish for mass communication, and dedicated academic research to it. We now wish, in addition, integrity, authentication, privacy, non-repudiation, fairness, access control, timestamping and more.

1.2 Terminology