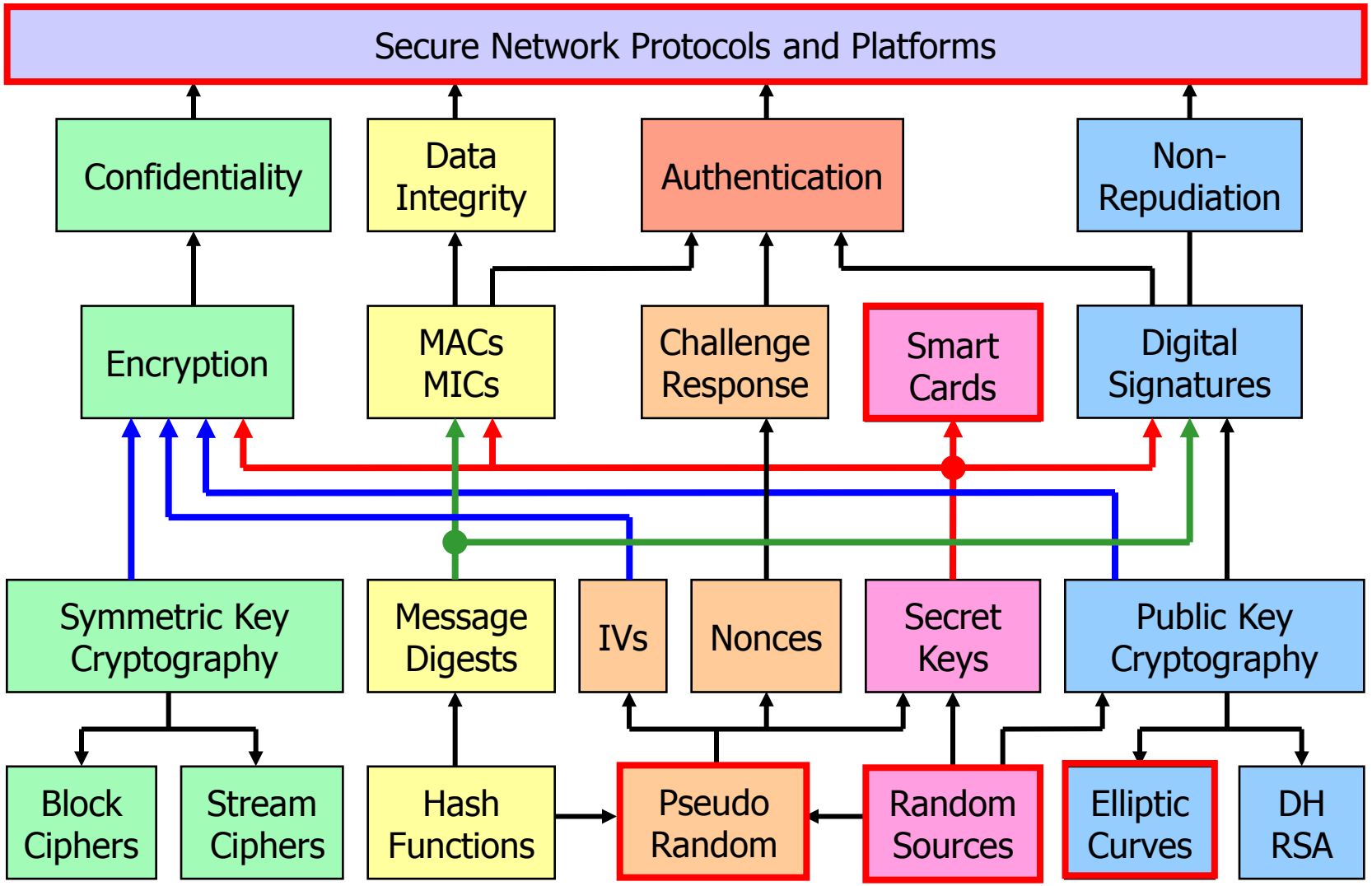
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

Overview

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

Cryptographical Building Blocks



Security Protocols for the OSI Stack

Communication layers	Security protocols
Application layer	Platform Security, Web Application Security, VoIP Security, SW Security
Transport layer	TLS
Network layer	IPsec
Data Link layer	[PPTP, L2TP], IEEE 802.1X, IEEE 802.1AE, IEEE 802.11i (WPA2)
Physical layer	Quantum Cryptography

Agenda of "InfSi2 – Network & Platform Security"

18.09.13	Overview, Constant Cryptographic Strength, Elliptic Curves
25.09.13	Physical Layer Security (Quantum Crypto, Random Numbers)
2.10.13	Link Layer Security (MAC, WLAN, 3G/4G, 802.1X, RADIUS)
9.10.13	Network Layer Security (Virtual Private Networks, IPsec)
16.10.13	Network Layer Security (Internet Key Exchange)
23.10.13	Network Layer Security (DNSSEC)
30.10.13	Session Layer Security (VoIP Security via SRTP, MIKEY)
6.11.13	Network Anonymity (Mix Chains, Tor)
13.11.13	Network Access Control (Firewalls, Intrusion Detection/Prevention)
20.11.13	Network Access Control (Trusted Network Connect)
27.11.13	Platform Security Threats (Buffer Overflows, Rootkits)
4.12.13	Platform Security (Smartcards, Hardware Security Modules)
11.12.13	Platform Security (Trusted Platform Module, Attestation)
18.12.13	Platform Security (Virtualization, Separation)

Recommended Literature – Network Security

- William Stallings,
  Network Security Essentials,
  Fifth Edition,
  International Edition,
  448 pages, 2013,
  Pearson Education, Inc.,
  ISBN 0-27-379336-5

  41 € @ amazon.de