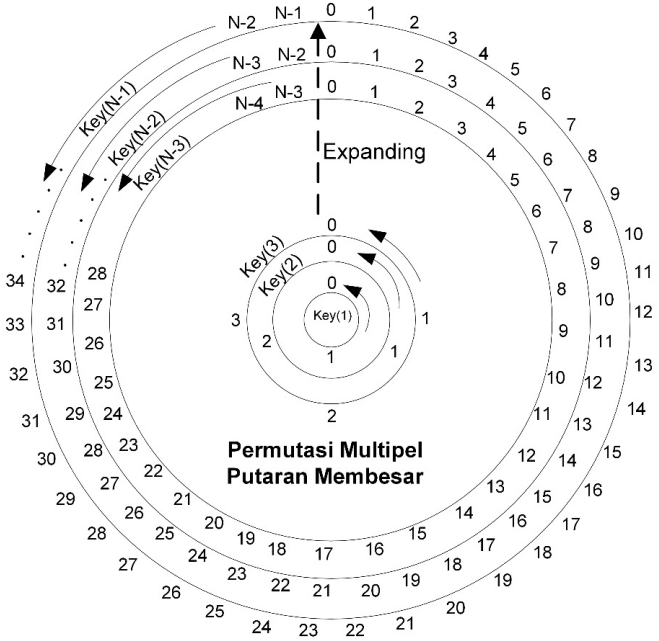

Dr. Yohan Suryanto, S.T, M.T

Semester Ganjil 2020/2021

Kriptografi 1
Pengantar

Outline

1. Dosen Pengampu
2. Jadwal Perkuliahan
3. Assesment
4. Tujuan Perkuliahan
5. Syllabus
6. Referensi

Dr. Yohan Suryanto, St. MT related certificated on cyber security:

1. CEI (Certified EC-Council Instructor)
2. CNSP (CompTIA Security Network Professional)
3. CNVP (CompTIA Network Vulnerability Assessment Professional)
4. ECSA (EC-Council Certified Security Analyst)
5. CompTIA Pentest+ (CompTIA PenTest+ ce Certification)
6. CompTIA CSAP (CompTIA Security Analytics Professional)
7. CTIA (EC-Council Certified Threat Intelligence Analyst)
8. CEH Master (EC-Council CEH Master)
9. CEH Practical (EC-Council CEH Practical)
10. CompTIA CySA+ (CompTIA CySA+ ce Certification)
11. CEH (EC-Council Certified Ethical Hacker)
12. CompTIA Security+ (CompTIA Security+ ce Certification)
13. CND (EC-Council Certified Network Defender)
14. CCNA (Cisco Certified Network Associate)
15. HCAI (Huawei Certified Associate Instructor)
16. HCIA RS (Huawei Certified ICT Associate Routing and Switching)
17. HCAI (Huawei Certified Academy Instructor)

Jadwal Perkuliahan

- Perkuliahan 14 September 2020 – Januari 2021
- UTS November
- UAS Januari 2021
- Ujian perbaikan -
- Pembagian Daftar Nilai Sebelum Februari 2021

Assessment

- Grading :
  - Assignment : 30 % 10%
  - UTS : 30 % 10%
  - UAS/ Project : 40 % 15%
    : 30%
    : 35%

Tujuan Perkuliahan

- Mahasiswa memahami konsep kriptografi, dasar-dasar kriptanalisis, dan implementasinya untuk pengamanan sistem informasi.

Syllabus

1. Pendahuluan
2. Pengenalan Matlab / Octave
3. Dasar-dasar matematika kriptografi
4. Algoritma Kriptografi klasik
5. Dasar-dasar Kriptanalisis
6. Matematika Kriptografi Struktur Aljabar
7. Algoritma symmetric key modern AES
8. Hashing
9. Distribusi Symmetric key

Referensi

- Forouzan, Behrouz A., and Debdeep Mukhopadhyay. *Cryptography and Network Security (Sie)*. McGraw-Hill Education, 2011.
- Stallings, William. "Cryptography and Network Security. 2005." *ISBN: 0-13-187316-4*.
- Attaway, Stormy. *Matlab: a practical introduction to programming and problem solving*. Butterworth-Heinemann, 2013.
- Hoffstein, Jeffrey, et al. *An introduction to mathematical cryptography*. Vol. 1. New York: springer, 2008.
- Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press, 1996.
- Stinson, Douglas R. *Cryptography: theory and practice*. CRC press, 2005.