

# Introduction to Computer Forensics and Security (6G7Z1009\_1819\_9Z6)

## Reading list

### Book Chapters:

1. N. Ferguson, B. Schneier, T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, (1st Edition) 2010, John Wiley.
2. W. Stallings, Cryptography and Network Security: Principles and Practice (5th Edition), 2010, Printice Hall (Chapter 2 and 3)
3. M. Stamp, Information Security. Principles and Practice (2nd Edition), 2011, John Wiley. (Chapter 2 and 3)
4. Alexander Stanoyevitch, Introduction to Cryptography with Mathematical Foundations and Computer Implementations, 2010, CRC Press ( Chapter 7)
5. J. Erickson, Hacking: The Art of Exploitation (2nd Edition), 2008 (Chapter 7)

### Online resources:

The Vernam Cipher, [www.cryptomuseum.com/crypto/vernam.htm](http://www.cryptomuseum.com/crypto/vernam.htm), [Online access 10 Sep. 2014]. Neal R. Wagner, The Laws of Cryptography: Perfect Cryptography: The One-Time Pad, [www.cs.utsa.edu/~wagner/laws/pad.html](http://www.cs.utsa.edu/~wagner/laws/pad.html), [Online 10 September 2014].

Last modified: Friday, 24 October 2014, 3:17 PM