Homework

1. Describe BEAST attack scenario in detail, which is the chosen-plaintext attack on CBC mode in TLS 1.0 (or prior SSL versions), to decrypt a message byte-by-byte
   - J. Rizzo, T. Duong, “Here come the XOR ninjas”, May 2011

- Base papers:
  - G.V. Bard, “The vulnerability of SSL to chosen plaintext attack”, IACR Cryptology, ePrint Archive 2004, May 2004
  - G.V. Bard, “A challenging but feasible blockwise-adaptive chosen-plaintext attack on SSL” In: SECRYPT 2006, Proceedings of the International Conference on Security and Cryptography, 2006

- This also may help
  - T. Kurokawa, R. Nojima, S. Moriai, “On the security of CBC Mode in SSL3.0 and TLS1.0”, JISIS, vol. 6, no. 1, 2016

Homework

2. Find the countermeasure fixed in TLS 1.1, and demonstrate why this is the case (how it can solve the vulnerability)
   - RFC 4346 (The Transport Layer Security (TLS) Protocol Version 1.1)
   - https://www.ietf.org/rfc/rfc4346.txt

- Due date
  - 2017. Nov. 6, 23:59
  - Upload your answer into the Blackboard