105學年上學期 專題報告

專題生 江昶翰 b03902060

1.read paper:

- Here come the xor ninja: http://netifera.com/research/beast/beast_DRAFT_0621.pdf

- This POODLE Bites Exploiting The SSLv3 fallback: https://www.openssl.org/~bodo/ssl-poodle.pdf

- A CHALLENGING BUT FEASIBLE BLOCKWISE-ADAPTIVE CHOSEN-PLAINTEXT ATTACK ON SSL : https://eprint.iacr.org/2006/136.pdf

2. other knowledge :

- RSA security

  (1)some algorithm to solve DLP，ex: Baby's and Giant's step, Pohlig–Hellman Algorithm

  (2)some algorithm to do integer factorization ,ex: Pollard's method,The Quadratic Sieve ,The Number Field Sieve, The Index Calculus Method

- tool of demonstration MITM , ex: mitm proxy

3.others effort

- try to understand beast attack and write my own code to demonstrate it ,but I have stock for a long while.