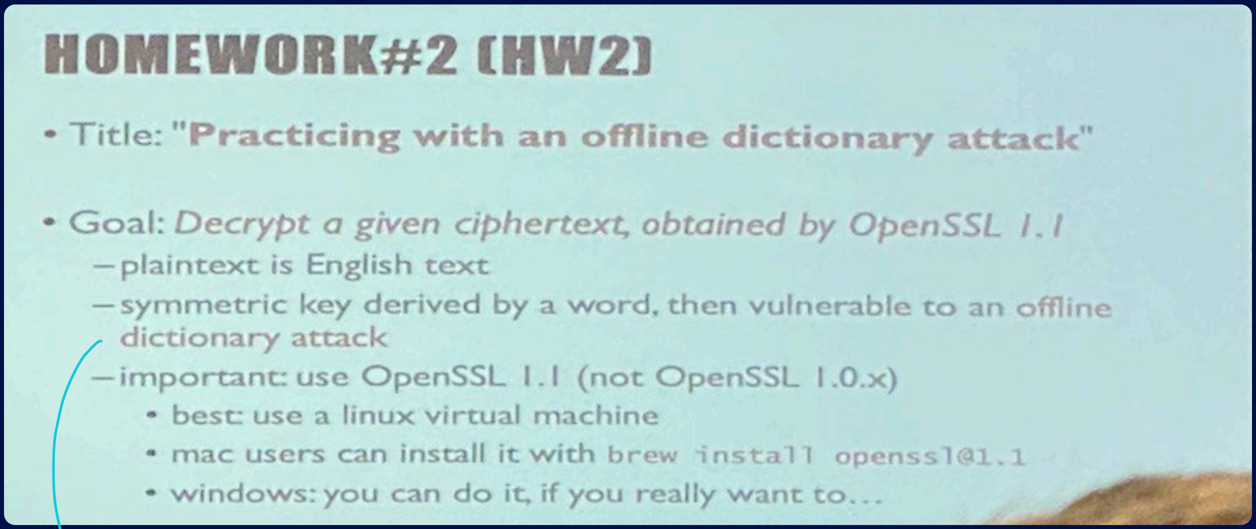
HOMEWORKS

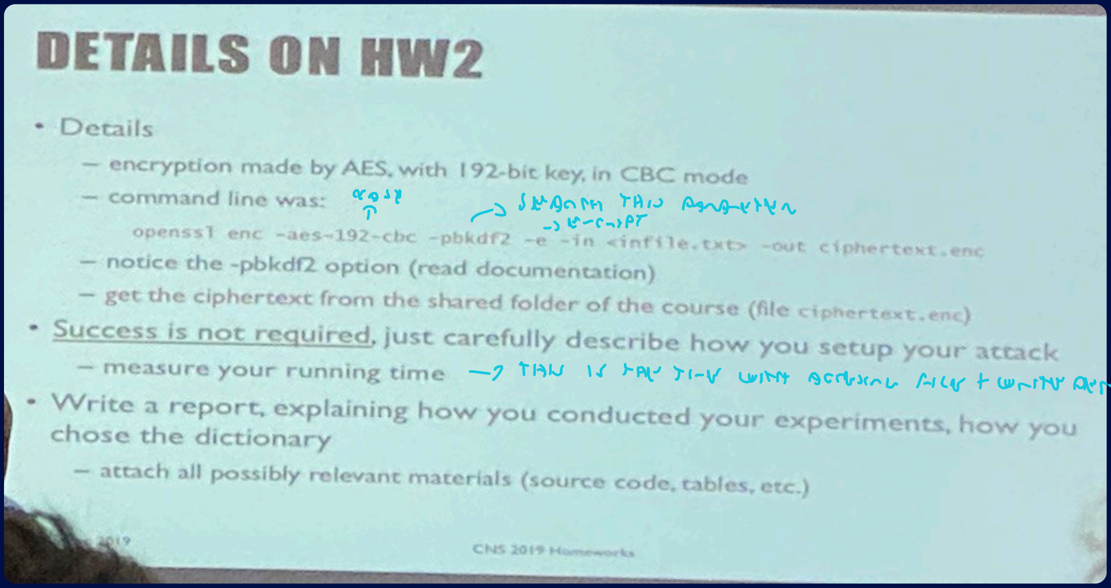


HOMEWORK#2 (HW2)

- Title: "**Practicing with an offline dictionary attack**"
- Goal: *Decrypt a given ciphertext, obtained by OpenSSL 1.1*
  - plaintext is English text
  - symmetric key derived by a word, then vulnerable to an offline dictionary attack
  - important: use OpenSSL 1.1 (not OpenSSL 1.0.x)
    - best: use a linux virtual machine
    - mac users can install it with `brew install openssl@1.1`
    - windows: you can do it, if you really want to...

ATTAK: ADV. ALL THE INFO (NOT PLAINTEXT AND KEY), SO WE TRY THE DECRYPTION STARTING FROM A WORD BY CHOOSING A COLLECTION OF WORDS (DICTIONARY)

– CHOOSE THE DICTIONARY THAT YOU WANT



DETAILS ON HW2

- Details
  - encryption made by AES, with 192-bit key, in CBC mode
  - command line was: [illegible] → SEARCH THIS PARAMETER

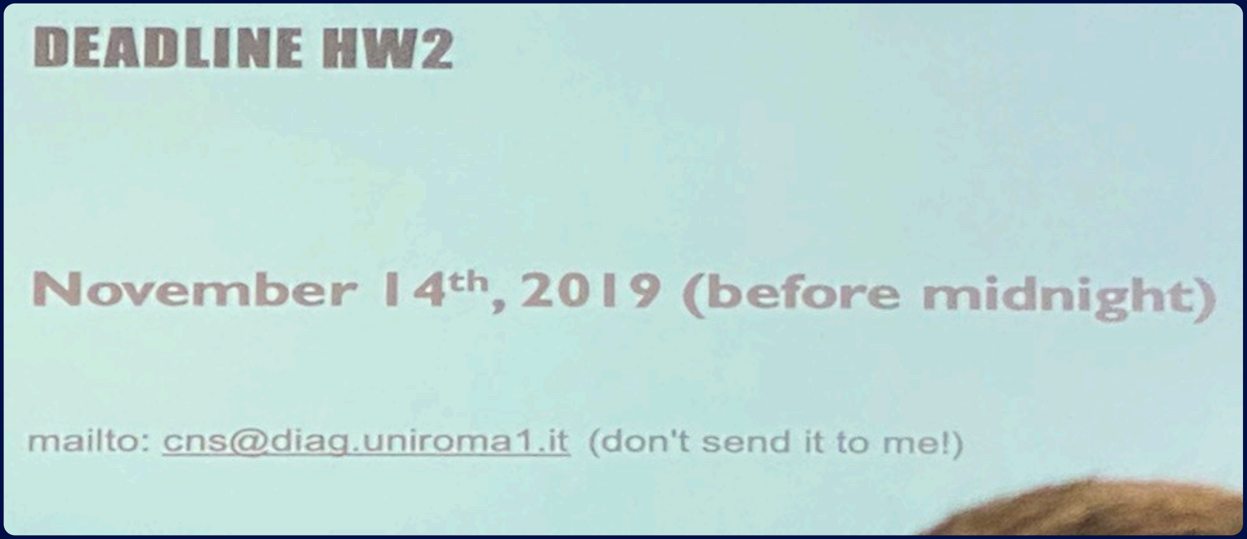
```
openssl enc -aes-192-cbc -pbkdf2 -e -in <infile.txt> -out ciphertext.enc
```

→ ENCRYPT

  - notice the -pbkdf2 option (read documentation)
  - get the ciphertext from the shared folder of the course (file ciphertext.enc)
- Success is not required, just carefully describe how you setup your attack
  - measure your running time → THIS IS THE TIME WITH [illegible] FILE + WRITE DETAIL.
- Write a report, explaining how you conducted your experiments, how you chose the dictionary
  - attach all possibly relevant materials (source code, tables, etc.)

2019

CNS 2019 Homeworks



DEADLINE HW2

November 14th, 2019 (before midnight)

mailto: cns@diag.uniroma1.it (don't send it to me!)