Université Gustave Eiffel

ESIEE PARIS

TP - Timing attacks

revision 1.1

Aim

Leak the secret.

Steps :

1. Download the code and pick a language (you can use either python or C/C++)
2. (Compile and) run the source code template
3. Read the source code and the rules inside
4. Find the issue in the code
5. Adapt the template to leak the secret. Start with a small 'length'.
6. Reduce 'slowness' as much as you can, and try to still leak the secret.

References

https://en.wikipedia.org/wiki/Timing_attack