Treball de Final de Grau “Enginyeria Informàtica”

Curs 2017-2018

Rendiment dels algorismes de xifratge en Embedded Systems mitjançant un HSM (Hardware Security Module)

Alumne: Joan Canals Mascorda  
Tutor: David Gómez Alari  
Universitat Rovira i Virgili  
ETSEI  
[joancanals95@gmail.com](mailto:joancanals95@gmail.com)

Índex del Treball

[1. Abstract 3](#_Toc519263410)

[2. Preàmbul 4](#_Toc519263411)

[I. Introducció 4](#_Toc519263412)

[II. Motivació personal 4](#_Toc519263413)

[3. Especificació tècnica dels dispositius 5](#_Toc519263414)

[I. Raspberry Pi 3B Plus 5](#_Toc519263415)

[II. HSM 5](#_Toc519263416)

[III. Dispositiu Android 5](#_Toc519263417)

[4. Llenguatges, funcionament i fragments de codi 6](#_Toc519263418)

[I. Raspberry 6](#_Toc519263419)

[II. HSM 6](#_Toc519263420)

[III. Android APP 6](#_Toc519263421)

[5. Criptosistemes utilitzats 7](#_Toc519263422)

[**I.** **AES** 7](#_Toc519263423)

[Descripció 7](#_Toc519263424)

[Perquè AES? 7](#_Toc519263425)

[Funcionament AES 7](#_Toc519263426)

[II. 3DES 10](#_Toc519263427)

[III. Camellia 10](#_Toc519263428)

[6. Estudi 11](#_Toc519263429)

[7. Conclusions 12](#_Toc519263430)

[8. Bibliografia i Webgrafia 13](#_Toc519263431)

[9. Paraules clau 14](#_Toc519263432)

[10. Annex 15](#_Toc519263433)

[I. Especificació tècnica dels dispositius 15](#_Toc519263434)

[i. Raspberry Pi 3B Plus 15](#_Toc519263435)

1. Abstract
   1. *words, in Engish.*
2. Preàmbul
   1. Introducció

La intenció d’aquest treball de final de grau és veure i estudiar el rendiment d’un sistema encastat alhora d’encriptar i desencriptar fitxers de diferents dimensions i extensions, utilitzant els recursos primaris del mateix sistema, comparant-ne els resultats obtinguts amb un seguit de dades de les operacions d’un xip **HSM**[[1]](#footnote-1) dedicat especialment a dur aquest tipus de tasques.

Ambdós tests realitzen el mateix càlcul amb el mateix fitxer. La qüestió és veure i poder analitzar quant és realment necessari disposar d’un xip dedicat per a realitzar depenent de quines encriptacions, i el nivell d’estrès que pot arribar a suportar un sistema encastat quan se li demana encriptar fitxers de grans dimensions.

Aquests tipus de sistemes encastats utilitzen sistemes d’encriptació lleugers, o *‘****Lightweight cryptosystems****’*, últimament en més ús i en ple desenvolupament gràcies al **IoT**.

* 1. Motivació personal

La motivació personal que m’ha fet escollir aquest treball de fi de grau ve marcada pel fet que durant la realització de la carrera em van cridar molt l’atenció dues assignatures que mostraven dos camps diferenciats dins del món de la informàtica: el camp de la seguretat informàtica; i el camp dels sistemes encastats.

Així doncs, i gràcies a un encaminament adient del meu tutor del treball de final de grau, vaig decidir fer un estudi que engloba els dos camps, podent així interpretar-los i aprofundir-los en més detall.

També he decidit fer-ho d’aquests camps perquè m’agradaria seguir aprofundint en aquestes matèries, on he trobat la motivació adient.

1. Especificació tècnica dels dispositius

A continuació hi ha una breu descripció[[2]](#footnote-2) dels dispositius emprats durant la realització de l’estudi, per a poder justificar les dades obtingudes. En aquesta especificació es mostra la dimensió de la memòria de cada dispositiu i la freqüència a la que treballa la seva pròpia CPU.

* 1. Raspberry Pi 3B Plus

Sistema encastat que ha estat utilitzat per a realitzar l’estudi, aquí una molt breu descripció tècnica del dispositiu:

* Processador: Broadcom BCM2837B0, Cortex-A53 64-bit SoC.
* Freqüència del processador: 1.4 GHz
* Memòria: 1GB LPDDR2 SDRAM
  1. HSM
  2. Dispositiu Android

1. Llenguatges, funcionament i fragments de codi
   1. Raspberry
   2. HSM
   3. Android APP
2. Criptosistemes utilitzats

Els criptosistemes utilitzats per a la realització de l’estudi han estat els criptosistemes més lleugers, o semblants al tipus de ‘*Lightweigth cyrptosystems*’ que l’eina *OpenSSL[[3]](#footnote-3)* ha pogut proporcionar. Aquests criptosistemes són els següents.

* 1. **AES**

Descripció

L’AES o Advanced Encryption Standard, és una especificació per al procés d’encriptació de dades establerta per l’Institut Nacional d’Estàndards i Tecnologia (NIST) l’any 2001.

AES està basat en un principi de disseny conegut com a *‘xarxa de substitució-permutació’*, i funciona igual de ràpid ja sigui implementat via Software o via Hardware. Aquest criptosistema té una mida bloc de 128 bits, o *Block Size*, i té una dimensió variable de 128, 192 o 256 bits de la clau, o *Key Size*.

Perquè AES?

L’elecció de l’AES ve marcada per la seva semblança amb el criptosistema PRESENT, aquest últim és un xifrador *ultra-lightweight* recomenat en l’estàndard ISO/IEC 29192-2 per a l’ús en aplicacions criptogràfiques *lightweight*, concretament el mateix tipus d’aplicacions que s’intenta reproduir en aquest estudi.   
Tot i que el PRESENT també és un criptosistema de bloc, la principal diferencia entre aquest i l’AES és la diferència de dimensió de bloc, PRESENT disposa d’un bloc de 64 bits i el de l’AES és de 128 bits.

Una de les altres grans semblances però alhora també s’esdevé una nova diferència és l’ús de mòduls d’encriptació o *caixes[[4]](#footnote-4)* que utilitzen els dos sistemes, AES utilitza una substitució complexa de *caixes*, mentre que el PRESENT té un mètode reduït de substitució per *caixes*. Així doncs, l’AES és considerat un mètode molt vàlid i eficaç per implementacions tant en Software com en Hardware, mentre que el PRESENT és una opció per a encriptació *ultra-lightweight* particularment eficient per a implementacions Hardware.

Aquests dos criptosistemes disposen de diverses característiques en comú que fan possible una igual caracterització en una plataforma mòbil *Smartphone*, o en un *Embedded System*.

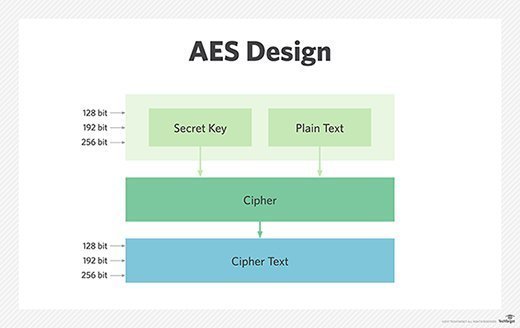
Funcionament AES

AES es basa en un principi de disseny conegut com a xarxa de *substitució-permutació*. Com hem dit abans, utilitza 128 bits per la dimensió de la clau i una dimissió variable de 128, 192 o 256 bits per a la clau, ambdós valors sempre múltiples de 32 bits. Aquest sistema de xifratge és simètric, això significa que utilitza la mateixa clau per encriptar que per desencriptar, així tant l’emissor com el receptor coneixen i utilitzen la mateixa clau secreta.

AES opera amb matrius de bytes de 4 x 4, anomenades matrius *State*. Com s’ha dit abans, AES utilitza *caixes* que venen a ser els camps de la matriu, en cada matriu hi ha un total de 16 *caixes*.

La dimensió de la clau utilitzada especifica el nombre de rondes de transformació que converteixen el text pla, o d’entrada, en un text xifrat. El nombre de rondes és el següent:

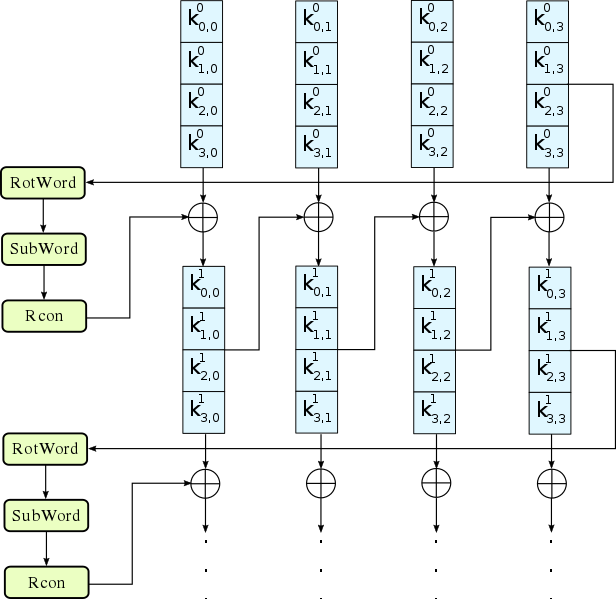
* 10 rondes per una clau de dimensió de 128 bits.
* 12 rondes per una clau de dimensió de 192 bits.
* 14 rondes per una clau de dimensió de 256 bits.

[[5]](#footnote-5)

Pas inicial – Key Expansion

El model segueix la metodologia *Rijndael Key Schedule[[6]](#footnote-6)* que fa ús de les *Rijndael S-box*. La *S-box* és la *caixa de substitució*, que serveix com una *lookup table*, que s’agafa de la matriu *State.*

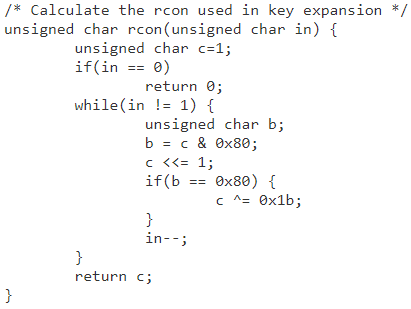
Una imatge gràfica del *Rijndael Key Schedule*:

[[7]](#footnote-7)

El primer pas consisteix en expandir una clau primària introduïda, de 128 bits, en aquest cas, en una clau final anomenada *Round Key* de 128 bits, que serà utilitzada per a l’encriptació; i això és fa seguint el següent conjunt de procediments de la tècnica *Rijndael Key Schedule*:

Per expandir una clau de 128 bits, s’utilitza una matriu de 176 bytes, per Sistemes Encastats i targetes Intel·ligents sense aquesta quantitat de RAM s’utilitza una matriu adaptada que no consumeix tanta memòria.

1. Els primers 16 bytes de la *expanded key* són els 16 bytes de la clau d’encriptació inicial.
2. A continuació es posa la variable *i* per a l’opearció *rcon* a 1.  
   L’operació *rcon* és una exponenciació de l’ordre de 2, escrita amb el llenguatge C seria la següent:



Transformacions

La primera transformació en l’encriptació AES és la substitució utilitzant una taula de substitució, això s’aconsegueix combinant cada *caixa* de la matriu amb un bloc de la clau utilitzant l’operació XOR.

Les següents 9, 11 o 13 rondes de transformació, depenent de la clau, es mouen i intercanvien files, barrejant-ne les dades, la tercera barreja les columnes. La última transformació és l’operació d’una XOR executada en cada columna utilitzant una part diferent de la clau, per tant una clau més llarga necessita més rondes per a ser completada.

* 1. 3DES
  2. Camellia

1. Estudi
2. Conclusions
3. Bibliografia i Webgrafia

* Web oficial de Zymbit, per a la compra del mateix i les especificacions tècniques i de la utilització de la API:  
  <https://www.zymbit.com/keys-to-security-raspberry-pi/>
* Fòrum oficial de Raspberry Pi, per a la consulta d’informació tècnica i resolució de bugs:  
  <https://www.raspberrypi.org/forums/>
* Fòrum d’Stack Overflow, per a la consulta de comandes Android i algunes comandes de Python:  
  <https://stackoverflow.com>
* La pàgina de Wikipedia per a la consulta de sigles i recerca d’informació:  
  <https://en.wikipedia.org/>
* La pàgina d’OpenSSL per a informació i fòrum d’ajuda:  
  <https://www.openssl.org>
* Informació addicional sobre el funcionament de l’AES: <https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>
* Document ‘*An evaluation of AES and PRESENT ciphers for lightweight cryptography on smartphones*’ – Centro de Investigación y Estudios Avanzados de IPN, Laboratorio de Tecnologías de Información; per acreditar l’ús del criptosistema AES.
* Per a l’explicació del funcionament del AES:  
  <https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf>
* Youtube per a vídeos explicatius i exemples gràfics:  
  <https://www.youtube.com>

1. Paraules clau

**AES:** Advanced Encryption Standard, és un criptosistema simètric de xifratge de bloc, definit per la NIST.

**HSM:** Hardware Security Module, o mòdul de seguretat dedicat, és el Hardware que desenvolupa les tasques dedicades d’encriptació i desencriptació.

**IoT:** Internet of Things o Internet de les Coses.

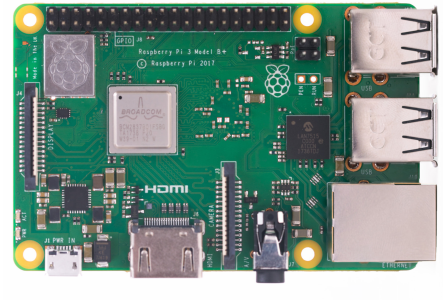
**Lightweight cryptography:** Criptosistemes lleugers, són els criptosistemes que pretenen actuar com un sistema d’encriptació i desencriptació normal, utilitzant menys recursos i sent igual o millor d’eficaços i eficients.

**NIST:** National Institute of Standards and Technology.

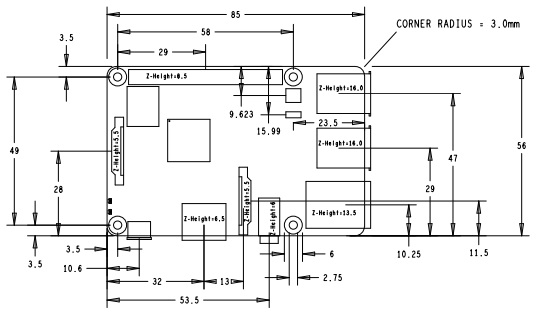
**TLS:** Transport Layer Security, o protocol de seguretat en la capa de transport.

**SSL:** Secure Sockets Layer, o protocol d’encriptació de sockets per a comunicacions segures.

1. Annex
   1. Especificació tècnica dels dispositius
      1. Raspberry Pi 3B Plus

**[[8]](#footnote-8)**

* **Resum**
  + Processor: Broadcom BCM2837B0, Cortex-A53 64-bit SoC @ 1.4 GHz
  + Memory: 1GB LPDDR2 SDRAM
  + Connectivity:
    - 2.4 GHz i 5 GHz IEEE 802.11 .b/g/n/ac wireless LAN, Bluetooth 4.2, BLE
    - Gigabit Ethernet over USB 2.0 (maximum throughput 300 Mbps)
    - 4 x USB 2.0 ports
  + Access: Extended 40-pin GPIO header
  + Video & Sound:
    - 1 x full size HDMI
    - MIPI DSI display port
    - MIPI CSI càmera port
    - 4 pole stereo output and composite vídeo port
  + Multimedia: H.264, MPEG-4 decode (1080p30); H.264 encode (1080p30); OpenGL ES 1.1, 2.0 graphics
  + SD card suport: Micro SD format for loading operating System and data storage
  + Input power:
    - 5V/2.5A DC via micro USB connector
    - 5V DC via GPIO header
    - Power over Ethernet (PoE) – enabled (requires separate PoE HAT)
  + Environment: Operating temperature, 0 – 50ºC
* **Especificacions físiques**

**[[9]](#footnote-9)**

1. Tota paraula en negreta té la seva explicació i/o traducció en l’apartat *‘9. Paraules Clau’*. [↑](#footnote-ref-1)
2. A l’apartat d’Annex hi ha un seguit de fotografies dels dispositius i també consta de les especificacions físiques més detallades. [↑](#footnote-ref-2)
3. És un *Toolkit* per als protocols TLS i SSL. És una llibreria d’encriptació de propòsit general. OpenSSL està llicenciat sota una llicència *Apache*. [↑](#footnote-ref-3)
4. Terme metafòric per a referir-se a una part de la matriu. [↑](#footnote-ref-4)
5. Imatge extreta de la web: <https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard> [↑](#footnote-ref-5)
6. En el món de la criptografia, hi ha *xifradors del producte*, o *product ciphers*, els quals per xifrar i desxifrar les dades ho fan utilitzant iteracions, o *rounds*. Un *Key Schedule* és un algoritme que calcula la clau resultant per una clau primària introduïda a base d’iterar i aplicar un algorisme sobre la primera clau. [↑](#footnote-ref-6)
7. Imatge extreta de la web: <https://en.wikipedia.org/wiki/Rijndael_key_schedule> [↑](#footnote-ref-7)
8. Imatge extreta de la web: <https://static.raspberrypi.org/files/product-briefs/Raspberry-Pi-Model-Bplus-Product-Brief.pdf> [↑](#footnote-ref-8)
9. Imatge extreta de la web: <https://static.raspberrypi.org/files/product-briefs/Raspberry-Pi-Model-Bplus-Product-Brief.pdf> [↑](#footnote-ref-9)