În ceea ce privesc rezultatele de performanță pentru aplicațiile individuale din cadrul acestei lucrări s-au făcut teste în urma cărora s-au urmărit timpii de execuţie ai algoritmului RSA atât în ceea ce privește numai criptarea cât și în ceea ce privește criptarea urmată de decriptare. Aplicațiile au fost rulate în paralel pe platforma QorIQ P1025E şi pe o platformă x86. Platforma x86 foloseşte un core la 2,2 GHz, pe când plăcuţa foloseşte un core la 500 MHz. În cazul aplicaţilor propuse, platforma foloseşte un singur core din componenţa ei pentru rularea aplicaţiei şi nu foloseşte accelerarea hardware existentă. Timpii de execuţie a aplicaţiilor rulate pe platformă vor fi mai mari, însă consumul de putere ar fi situat la un raport de 5 wați în cazul platformei QorIQ P1025E la 70 wați în cazul platformei x86.

În cadrul acestor teste în funcție de lungimile cheilor de 1024,2048 respectiv 4096 biți s-a ținut cont de dimensiunea cadrului de 16,64,128,256,512,936,1024,1960, 2048 și 4008 exprimat în biți care urmează să fie criptat și decriptat. Conform implementării algoritmului de criptare RSA descris în paragraful 3.2.6 dimensiunea unui text în clar care urmează să fi criptat pentru testarea timpilor de execuție se limitează la următoarele valori:

* pentru setul de chei de 1024 biți,cadrul care urmează să fie criptat ≤ 117 octeți.
* pentru setul de chei de 2048 biți, cadrul care urmează să fie criptat ≤ 245 octeți.
* iar pentru setul de chei de 4096 biți, cadrul care urmează să fie criptat ≤501 octeți.

Rezultatele au fost redate în funcție de timp și de numărul de execuții, asfel încât acestea au fost exprimate în operații pe secundă.

Testarea pentru dimensiunea cheilor publice de 4096 biți

În urma rulării algoritmului de criptare RSA pe platforma Platforma x86 s-au obţinut

următorii timpi de execuţie:

|  |  |  |  |
| --- | --- | --- | --- |
| Platforma x86 2Gz  Criptare RSA key-4096 biți | | | |
| Dimensiune mesaj criptat[biți] | **Numărul de execuții** | **Timp execuție[secunde]** | **Criptare RSA**  **Operații pe secundă** |
| 16 | **1000** | **5,091 s** | **192,425 op/s** |
| 64 | **5,174 s** | **193,274 op/s** |
| 128 | **5,035 s** | **198,609 op/s** |
| 256 | **4,754 s** | **210,349 op/s** |
| 512 | **5,312 s** | **188,253 op/s** |
| 1024 | **5,690 s** | **175,746 op/s** |
| 2048 | **6,618 s** | **151,103 op/s** |
| 4008 | **5,718 s** | **174,889 op/s** |

|  |  |  |  |
| --- | --- | --- | --- |
| Platforma QorIQ P1025E 500MHz  Criptare și Decriptare RSA-2048 key | | | |
| Dimensiune mesaj criptat[biți] | **Numărul de execuții** | **Timp execuție[secunde]** | **Criptare+Decriptare**  **RSA**  **Operații/secundă** |
| 16 | **1000** | **177,188 s** | **5,643 op/s** |
| 64 | **192,278 s** | **5,200 op/s** |
| 128 | **270,758 s** | **3,693 op/s** |
| 256 | **276,409 s** | **3,617 op/s** |
| 512 | **258,578 s** | **3,860 op/s** |
| 1024 | **252,569 s** | **3,959 op/s** |
| 2048 | **253,880 s** | **9,938 op/s** |
| 4008 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Platforma x86 2Gz  Decriptare RSA key 2048 biți | | | |
| Dimensiune mesaj decriptat[biți] | **Numărul de execuții** | **Calculare timp necesar execuției**  **Decriptării [secundă]** | **Decriptare RSA**  **Operații /secundă** |
| 4096 | **1000** | **172,097 s** | **5,810 op/s** |
| 4096 | **187,104 s** | **5,344 op/s** |
| 4096 | **265,723 s** | **3,763 op/s** |
| 4096 | **271,655 s** | **3,681 op/s** |
| 4096 | **253,266 s** | **3,948 op/s** |
| 4096 | **246,879 s** | **4,050 op/s** |
| 4096 | **247,262 s** | **4,044 op/s** |

În urma rulării algoritmului în scopul realizării criptării RSA pe Platforma QorIQ P1025E s-au obţinut următorii timpi de execuție:

|  |  |  |  |
| --- | --- | --- | --- |
| Platforma QorIQ P1025E 500MHz  Criptare RSA key-4096 biți | | | |
| Dimensiune mesaj criptat[biți] | **Numărul de execuții** | **Timp execuție[secunde]** | **Criptare RSA**  **Operații/secundă** |
| 16 | **1000** | **24,589 s** | **40,660 op/s** |
| 64 | **24,631 s** | **40,599 op/s** |
| 128 | **24,582 s** | **40,680 op/s** |
| 256 | **24,569 s** | **40,701 op/s** |
| 512 | **24,535 s** | **40,758 op/s** |
| 1024 | **24,531 s** | **40,764 op/s** |
| 2048 | **24,416 s** | **40,956 op/s** |

În urma rulării algoritmului în scopul realizării criptării apoi a decriptării RSA pe Platforma QorIQ P1025E timpii de execuție sunt următorii:

|  |  |  |  |
| --- | --- | --- | --- |
| Platforma QorIQ P1025E 500MHz  Criptare și Decriptare RSA key-4096 biți | | | |
| Dimensiune mesaj criptat[biți] | **Numărul de execuții** | **Măsurare timp necesar execuție**  **Criptare+decriptare[s]** | **Criptare +Decriptare**  **RSA**  **Operații/secundă** |
| 16 | **1000** | **1613,406 s** | **0,61980 op/s** |
| 64 | **1614,018 s** | **0,61957 op/s** |
| 128 | **1612,392 s** | **0,62019 op/s** |
| 256 | **1612,593 s** | **0,62011 op/s** |
| 512 | **1612,400 s** | **0,62019 op/s** |
| 1024 | **1612,336 s** | **0,62021 op/s** |
| 2048 | **1612,290 s** | **0,62023 op/s** |

|  |  |  |  |
| --- | --- | --- | --- |
| Platforma QorIQ P1025E 500MHz  Decriptare RSA key 2048 biți | | | |
| Dimensiune mesaj decriptat[biți] | **Numărul de execuții** | **Calculare timp necesar execuției**  **Decriptării [secundă]** | **Decriptare RSA**  **Operații /secundă** |
| 4096 | **1000** | **1588,817 s** | **0,62939 op/s** |
| 4096 | **1589,387 s** | **0,62917 op/s** |
| 4096 | **1587,810 s** | **0,62979 op/s** |
| 4096 | **1588,024 s** | **0,62971 op/s** |
| 4096 | **1587,801 s** | **0,62980 op/s** |
| 4096 | **1587,805 s** | **0,62980 op/s** |
| 4096 | **1587,874 s** | **0,62977 op/s** |

Având o serie de rezultate în urma rulării se poate observa că din punct de vedere al timpilor de execuție setul de chei de 1024 biți oferă timpul cel mai convenabil, însă și setul de chei de 2048 biți prevede timpi de execuție în limita așteptărilor umane. RSA cu o dimensiune a cheilor de 4096 de biți pentru un număr mare de execuții nu prevede fiabilitate, însă trebuie specificat că oferă siguranța și confidențialitate de înaltă calitate.

În general RSA este prea lent pentru a cripta volume mari de date în mod eficient, dar este folosit la distribuția cheilor de sesiune în sistemele hibride.