Lightweight praktika

Data: 08/12/2024
Egileak: Oier Barrutiabengoa eta Gaizka Cerezo

Erabilitako hardwarea eta softwarea

Konpiladorean bertsioa: gcc (Debian 14.2.0-8) 14.2.0
CPUa: AMD Ryzen 7 4800H with Radeon Graphics (16 core logiko, 8 nukleo) (2,9GHz)

Hartutako erabakiak

Programak aztertzeko 1.000.000 enkripzio-dekripzio ziklo aztertu dira ref, opt64 eta opt64_lowsize programetan eta 100.000 enkripzio-dekripzio ziklo aztertu dira aes-GCM programean (denbora gehiegi behar duelako 1.000.000 ziklorekin). Programa guztietan 100 lehenengo zikloak ez ditugu kontuan hartu (berotze fasea). Azkenik bataz besteko denbora eta desbideratze estandarra kalkulatu ditugu programa guztietan.

Ref

ref	ENKRIPTAZIOA		DEKRIPTAZIOA	
	Bataz besteko denbora (us)	Desbideratze estandarra (us)	Bataz besteko denbora (us)	Desbideratze estandarra (us)
64 byte	0,337	0,330	0,677	0,328
128 byte	0,490	0,290	0,974	0,444
512 byte	1,357	0,517	2,723	0,616
1024 byte	2,503	0,712	5,304	1,114
2048 byte	4,802	0,937	9,824	3,473
4096 byte	9,514	2,356	19,126	3,423

Exekutagarriaren tamaina: 29KiB

Opt64

opt64	ENKRIPTAZIOA		DEKRIPTAZIOA	
	Bataz besteko denbora (us)	Desbideratze estandarra (us)	Bataz besteko denbora (us)	Desbideratze estandarra (us)
64 byte	0,237	0,246	0,47	0,323
128 byte	0,342	0,514	0,68	0,747
512 byte	0,931	0,709	1,861	1,037
1024 byte	1,724	1,331	3,479	1,913
2048 byte	3,261	0,902	6,603	1,299
4096 byte	6,395	1,264	12,932	1,812

Exekutagarriaren tamaina: 33KiB

Opt64_lowsize

opt64_lowsize	ENKRIPTAZIOA		DEKRIPTAZIOA	
	Bataz besteko denbora (us)	Desbideratze estandarra (us)	Bataz besteko denbora (us)	Desbideratze estandarra (us)
64 byte	0,291	0,226	0,579	0,353
128 byte	0,43	0,926	0,855	1,289
512 byte	1,235	1,142	2,414	1,665
1024 byte	2,26	1,055	4,415	1,432
2048 byte	4,411	3,246	8,617	4,795
4096 byte	8,479	3,251	16,55	4,623

Exekutagarriaren tamaina: 17KiB

Aes_GCM

aes_GCM	ENKRIPTAZIOA		DEKRIPTAZIOA	
	Bataz besteko denbora (us)	Desbideratze estandarra (us)	Bataz besteko denbora (us)	Desbideratze estandarra (us)
64 byte	55,046	5,243	110,1	7,827
128 byte	106,35	25,542	212,711	50,363
512 byte	384,14	81,416	768,12	161,19
1024 byte	750,265	144,102	1500,037	287,059
2048 byte	1435,595	202,284	2870,381	399,769
4096 byte	2777,538	190,483	5553,576	358,767

Exekutagarriaren tamaina: 21KiB

Tauletan ikusi daitekeen bezala ref, opt64 eta opt64_lowsize desberdintasun gutxi ikusi daitezke enkripzio eta dekripzio ezberdinen artean, aldiz Aes_GCM funtzioak erabiliz denbora askoz gehiago behar ditu enkriptatzeko eta dekriptatzeko.
Ref asconen bertsio estandarra da eta opt64 bertsioekin alderatuta exekutatzeko denbora gehien behar duen funtzioak ditu.
Opt64 ordenagailu 64 biteko arkitektura duten ordenagailuetarako pentsatuta dagoen funtzioak ditu eta honengatik azkarrena da.
Opt64_lowsize Opt64 bertsio optimizatua da, funtzioak exekutatzen denbora gehiago behar ditu baina tamaina txikiagoko exekutagarria sortzen du.
Azkenik Aes_GCM funtzio zaharrak erabiltzen dituen algoritmoak erabiltzen ditu eta oso motela da.

Konparazioak eta ondorioak

4096 Byte	ENKRIPTAZIOA (us)	DEKRIPTAZIOA (us)	TAMAINA (KiB)
Ref	9,514	19,126	29
Opt64	6,395	12,932	33
Opt64_lowsize	8,479	16,55	17
Aes_GCM	2777,538	5553,576	21

Emaitzak hobeto alderatzeko 4096 bytekin egindako proba hartzea erabaki dugu, ref eta opt bertsio ezberdinen artean enkriptatzerako orduan 2-3 mikrosegundoko ezberdintasuna dago, aldiz aes_GCM erabiltzean 2770 mikrosegundoko ezberdintasuna aurki dezakegu beste bertsio guztiekin alderatuta. Dekriptatzerako orduan ref, opt64 eta opt64_lowsize bertsioen artean 4-7 mikrosegundoko ezberdintasuna dago eta aes_GCM eta beste bertsioen arteko ezberdintasuna 5540 mikrosegundokoa da. Exekutagarrien tamainak konparatzean hoberena Opt64_lowsize da 17 KiBrekin Aes_GCM jarraitzen dio 21 KiBrekin eta azkenik ref 29 KiBrekin eta Opt64 33 KiBrekin ditugu. Emaitzak alderatuta enkripzioa eta dekripzioa azkar burutu nahi baldin badira orduan Opt64 erabiltzea gomendagarriagoa da, abiadura eta tamaina optimoak bilatu nahi baldin badira orduan Opt64_lowsize erabiltzea gomendagarriagoa da.