A mérések végzéséhez az alkalmazásomból elmentett adatokat fogom tesztadatként használni. Az adatokat struktúrált xml dokumentum formátumban kerülnek tárolásra. Három különböző méretű fájlt vizsgálunk. Reális méretű fájlok használatára törekedtem (~500KB, ~2MB ~4MB). Már a 4 MB nagyság (nem titkosított) elérését a program rendeltetésszerű használata esetén is elég valószínűtlen tartom, mivel nagyon sok random adatot kellett bemásoljak ahhoz, hogy elérjem ezt a fájlméretet.

Feltehető a mérési eredmények arányos növekedése nagyobb fájlméret esetén.

A mérések összeállítása előtti próbálgatásaimból megtudtam, hogy a titkosítási és visszafejtési idő (a program kód alapján, a System.currentTimeMillis() parancs használatával) nem mindig egyezik meg ugyanazon fájl többszöri titkosítása esetén. Ebből következik, hogy egy adott fájl titkosítását mindegyik algoritmus használatakor többször is el kell végeznem, hogy egy korrekt közelítő értéket kapjak.

A titkosítási algoritmusok alkalmazására javax.crypto kriptográfiai könyvtárat használtam.

<u>Korábban bemutatott szimmetrikus titkosítási algoritmusok összehasonlítása</u>:

	AES	DES	Triple DES	Blowfish
Lehetséges kulcs méret.	128/192/256	64 (56-ot használ)	Összesen 168 bit	Mérete 32 bittől 448 bit-ig terjedhet
Mekkora egy block mérete?	128 bit	64 bit	64 bit	64 bit
Matematikai algoritmus neve.	Rijndael cipher	Feistel cipher	Feistel cipher	Feistel cipher
Hány kört végez az algoritmus?	Kulcs mérettől függ 128 bit – 10 kör 192 bit – 12 kör 256 bit – 14 kör	16 kör	3 x 16 kör	16 kör
Külön kulcsot használ-e minden körben?	Igen, mindegyik kör más kulcsot használ.	Igen, különböző 48 bites kulcsokat.	Három különböző DES kulcs.	Igen, 32 bit nagyságúakat.
Sikerült-e már feltörni?	Nem.	Igen, úgynevezett brute force támadással.	Vegyes válaszokat találtam, de mivel már nem igazán használják csak régebbi szoftverek, és mivel a DES is fel lett törve, ezért valószínűleg **igen**.	Nem.

Úgy gondolom, hogy az algoritmusok biztonságával kapcsolatosan megfelelő méréseket nem tudok végezni, ezért nem szerepelnek a dokumentumban. Egyetlen hely, ahonnan információhoz juthatunk ezen a téren az internet. A táblázat 'Sikerült-e már feltörni' sorában lévő információk is az internetről vannak.

AES (Az összes táblázat értékei milliszekundumban (ms) értendőek)

500KB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	49	44	46	43	48	**46,2 ms**
Visszafejtés	7	7	6	7	7	**7,2 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	46	44	44	47	51	
Visszafejtés	7	8	7	8	8	

1MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	55	51	57	58	55	**54,2 ms**
Visszafejtés	13	12	11	12	12	**12 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	54	53	57	51	51	
Visszafejtés	12	12	11	12	13	

2MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	52	58	51	56	51	**56,7 ms**
Visszafejtés	18	17	17	17	17	**18 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	60	55	60	70	54	
Visszafejtés	20	18	20	18	18	

3MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	55	64	63	56	60	**61,1 ms**
Visszafejtés	20	22	21	21	21	**21,2 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	73	59	64	58	59	
Visszafejtés	23	21	20	22	21	

4MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	66	63	60	56	58	**63,2 ms**
Visszafejtés	23	23	22	23	22	**23 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	72	62	66	67	62	
Visszafejtés	24	24	23	23	23	

DES

500KB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	51	50	50	50	56	**54 ms**
Visszafejtés	17	21	17	16	17	**17,8 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	57	53	57	58	58	
Visszafejtés	18	16	20	17	19	

1MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	70	63	68	67	68	**67,7 ms**
Visszafejtés	29	30	30	31	30	**29,9 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	71	63	65	70	72	
Visszafejtés	31	32	29	27	30	

2MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	86	85	90	86	85	**88,6 ms**
Visszafejtés	48	47	48	48	48	**48,5 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	97	86	95	89	87	
Visszafejtés	49	49	50	49	49	

3MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	109	108	114	98	113	**110,5 ms**
Visszafejtés	68	67	67	68	69	**67,9 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	117	103	117	113	113	
Visszafejtés	67	68	67	70	68	

4MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	135	115	137	135	131	**132 ms**
Visszafejtés	84	85	83	83	83	**85 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	137	133	137	123	137	
Visszafejtés	91	84	86	88	83	

Triple DES

500KB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	73	69	70	74	71	**71,9 ms**
Visszafejtés	28	28	29	35	28	**30,4 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	74	74	74	70	70	
Visszafejtés	35	33	29	29	30	

1MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	105	98	109	102	110	**104,4 ms**
Visszafejtés	59	58	68	58	59	**59,3 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	106	102	105	107	100	
Visszafejtés	58	59	59	56	59	

2MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	149	148	157	149	145	**153,9 ms**
Visszafejtés	109	110	111	110	110	**115,7 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	161	166	153	157	154	
Visszafejtés	136	137	111	111	112	

3MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	205	216	241	209	204	**217,4 ms**
Visszafejtés	162	163	199	163	162	**174 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	209	238	206	242	204	
Visszafejtés	164	201	162	200	164	

4MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	258	254	258	255	303	**269,2 ms**
Visszafejtés	212	213	213	213	262	**229,1 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	262	263	310	259	270	
Visszafejtés	217	216	265	214	266	

Blowfish

500KB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	48	44	49	49	46	**48,6 ms**
Visszafejtés	14	13	12	13	13	**13,4 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	50	52	52	50	46	
Visszafejtés	12	14	15	14	14	

1MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	60	65	57	58	62	**59,2 ms**
Visszafejtés	18	21	18	19	21	**19,2 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	58	59	64	53	56	
Visszafejtés	18	20	20	18	19	

2MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	71	68	65	66	71	**69,8 ms**
Visszafejtés	32	33	32	32	32	**33 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	76	69	68	70	74	
Visszafejtés	33	35	35	32	34	

3MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	96	80	80	78	84	**82,7 ms**
Visszafejtés	41	41	42	42	41	**42,4 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	79	78	81	86	85	
Visszafejtés	45	42	43	42	45	

4MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	93	95	96	93	94	**93,7 ms**
Visszafejtés	51	53	52	50	40	**50,7 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	91	91	95	97	92	
Visszafejtés	54	52	52	51	52	

A fájl mérete titkosítás előtt és után minden esetben megegyezett, kivéve pár bájt különbséggel.

Titkosítás	**AES**	**DES**	**Triple DES**	**Blowfish**
500KB	46,2 ms	54 ms	71,9 ms	48,6 ms
1MB	54,2 ms	67,7 ms	104,4 ms	59,2 ms
2MB	56,7 ms	88,6 ms	153,9 ms	69,8 ms
3MB	61,1 ms	110,5 ms	217,4 ms	82,7 ms
4MB	63,2 ms	132 ms	269,2 ms	93,7 ms

Visszafejtés	AES	DES	Triple DES	Blowfish
500KB	7,2 ms	17,8 ms	30,4 ms	13,4 ms
1MB	12 ms	29,9 ms	59,3 ms	19,2 ms
2MB	18 ms	48,5 ms	115,7 ms	33 ms
3MB	21,2 ms	67,9 ms	174 ms	42,4 ms
4MB	23 ms	85 ms	229,1 ms	50,7 ms

A táblázat a mért átlagértékeket tartalmazza.

Volt néhány esetben viszonylag nagy eltérés az értékek között, például a Triple DES esetében, a 4MB méret 5.mérése ~50 milliszekundummal nagyobb mint a másik 4 mérés. Pontosabb átlagértékeket kaphatnánk, ha mondjuk az egyik módszerrel X méretű fájlt mondjuk százszor titkosítanánk, nem pedig csak tízszer, és az így kapott eredményeket átlagolnánk.

Ettől függetlenül az így kapott értékekről lehet következtetéseket vonni.

Mindkét téren (titkosítás és visszafejtés) az AES használata bizonyult a leggyorsabbnak. Ahogy a fájl mérete nőtt, úgy az AES titkosítási ideje nem nőtt olyan látványosan, mint a többi algoritmus esetében. Visszafejtési időre szintén igaz ez az állítás.

Gyorsaságot tekintve legközelebb az AES-hez a Blowfish állt, mind visszafejtés és titkosítás terén is.

A DES és a Triple DES közötti egyre inkább növekedő különbség várható volt, hiszen a Triple DES háromszor végzi el azt, amit a DES csak egyszer. Ennek ellenére titkosítási időben nem érte el a Triple DES az elődje háromszorosát, habár nagyobb fájlméret esetén a növekedésüket nézve valószínűleg el fogja, sőt ezt a tendenciát követve valószínűleg a különbség több, mint a háromszorosára is nőhet. Visszafejtési időben sokkal inkább látszik ez a különbség, 4 MB-os fájl titkosítása kétszer addig tart a Triple DES-nek, mint a simának, visszafejtést nézve 4 MB esetén ez az érték majdnem a háromszorosára nőtt.

A program szempontjából valószínűtlennek tartom a 4MB-nál nagyobb fájl lehetőségét, de a mérések kedvéért egy random 64MB nagyságú fájl titkosítását is elvégeztem ugyanilyen módon.

A kapott eredmények (szintén milliszekundumban értendők):

AES

65MB	1.mérés	2.mérés	3.mérés	4.mérés	5.mérés	Átlag
Titkosítás	392	369	359	411	364	**374,3 ms**
Visszafejtés	298	314	300	297	289	**307,2 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	377	354	374	377	366	
Visszafejtés	289	285	401	308	291	

DES

65MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	1678	1314	1703	1688	1676	**1576,6 ms**
Visszafejtés	1301	1272	1323	1297	1305	**1326,1 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	1681	1311	1328	1693	1694	
Visszafejtés	1309	1560	1297	1299	1298	

Triple DES

65MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	3505	3524	3522	3512	3515	**3597,6 ms**
Visszafejtés	3451	3464	3516	3452	3447	**3536,6 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	3514	3514	4351	3518	3501	
Visszafejtés	3438	3441	4269	3435	3453	

Blowfish

65MB	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	956	950	968	993	979	**985,4 ms**
Visszafejtés	735	775	755	762	747	**757,3 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	974	974	974	1089	997	
Visszafejtés	755	767	763	764	750	

Összegezve:

Titkosítás	**AES**	**DES**	**Triple DES**	**Blowfish**
65MB	374,3 ms	1576,6 ms	3597,6 ms	985,4 ms

Visszafejtés	**AES**	**DES**	**Triple DES**	**Blowfish**
65MB	307,2 ms	1326,1 ms	3536,6 ms	757,3 ms

Az előző 500KB-4MB-os táblázat 4MB-os értékeivel összehasonlítva ezeket az értékeket a következőt kapjuk:

Az AES titkosítási ideje 5,92-szeresére nőtt, amíg a visszafejtési ideje 13,35-szörösére.

A DES titkosítási ideje 11,94-szeresére nőtt, amíg a visszafejtési ideje 15,6-szorosára.

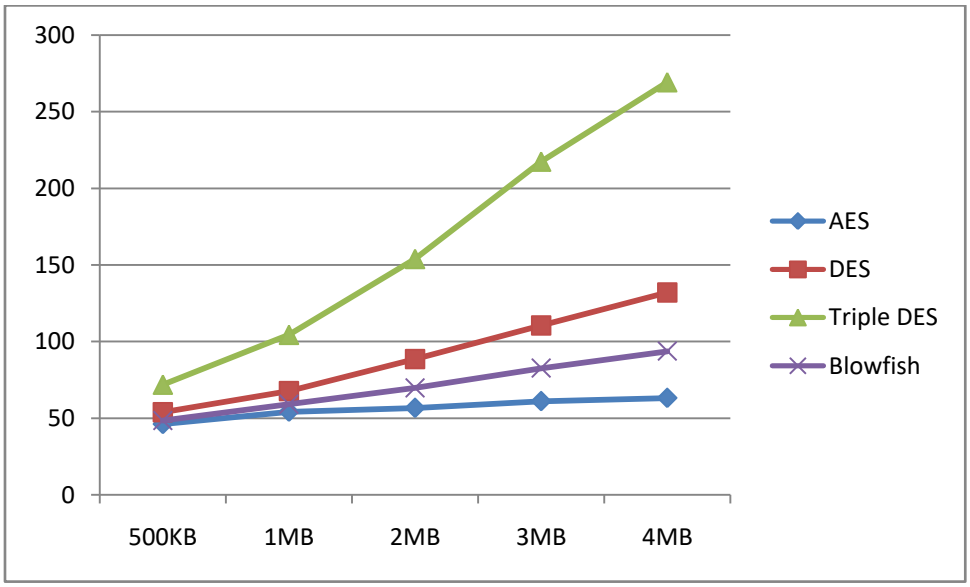
A TripleDES titkosítási ideje 13,36 -szorosára nőtt, amíg a visszafejtési ideje 15,44-szeresére.

A Blowfish titkosítási ideje 10,51-szeresére nőtt, amíg a visszafejtési ideje 14,94- szeresére.

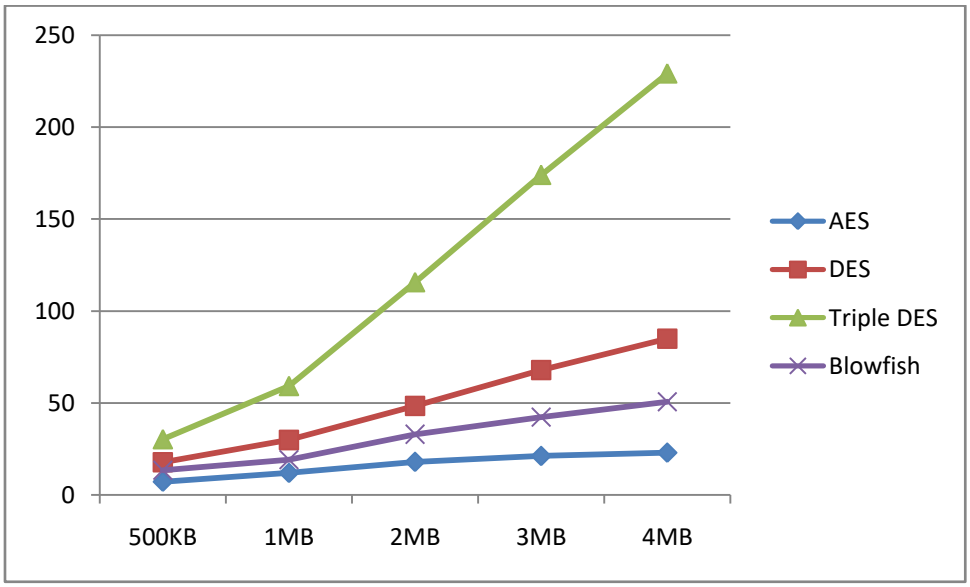
Ezek az adatok azért lehetnek érdekesek, mivel ha a 4MB és 64MB-os fájlméretet nézzük, akkor igaz, hogy 64 / 4 = 12, így ezt a logikát követve 12-szeres időnövekedést várhatunk titkosítás és visszafejtés esetén is. Ennek ellenére nem ezt kapjuk, hol többet, hol kevesebbet, tehát az egyenes arányosság logikáját nem követhetjük ebben az esetben.

Ezt az állítást egyébként igazolhatjuk az 500KB-4MB-os táblázatot nézve is, mivel ott sem pontosan duplázódtak meg az idők, annak ellenére, hogy a fájl mérete dupla akkora lett.

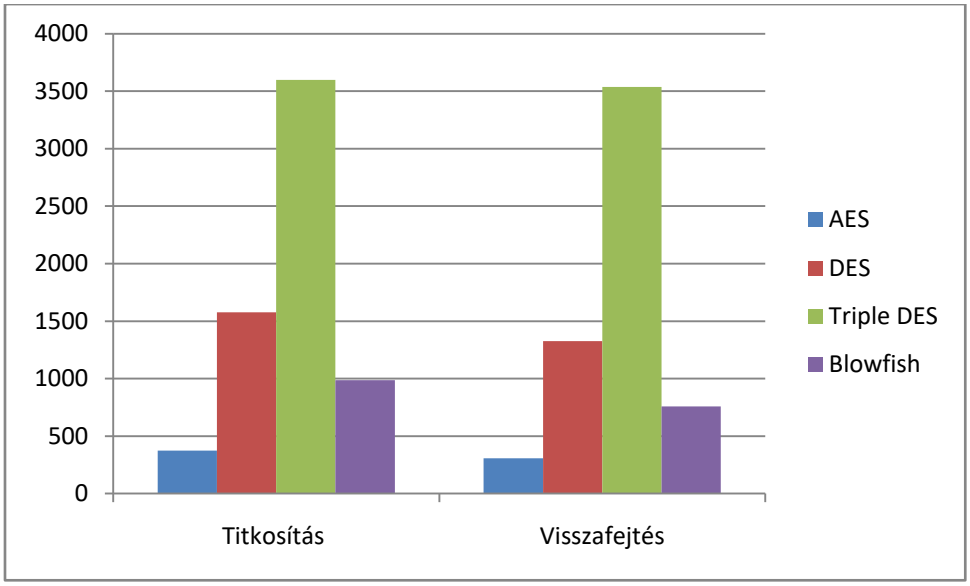
Titkosítás (függőleges tengely az eltel idő milliszekundumban, vízszintes a fájlméret):



Visszafejtés (függőleges tengely az eltelt idő milliszekundumban, vízszintes a fájlméret):



A 65 MB-os esetet külön diagramba rajzoltam, különben összenyomta volna az előző diagramok értékeit (függőleges tengely az eltelt idő milliszekundumban):



Aszimmetrikus titkosítási algoritmusok:

RSA

Szerettem volna a szimmetrikus algoritmusokkal összehasonlítani, de nem lenne korrekt, mivel az adatmennyiség felsőhatára, amit a javax.crypto könyvtár használatával titkosítani tudtam, az 245 byte volt. Ha nagyobb mérettel próbálkoztam ugyanazt a hibaüzenetet kaptam „Data must not be longer than 245 bytes”.

Ezután az interneten jobban utána olvastam a problémának és megtudtam, hogy az RSA algoritmus maximum akkora mennyiségű adatot képes titkosítani, mint az RSA kulcs mérete (mínusz az ún. header data, azaz fejlécadat).

Kettő hatványait használtam kulcsméret megadására, először 2048 byte nagyságú kulccsal kezdtem. A következő mérések ezzel készültek (szintén milliszekundumban értendők az értékek):

64 byte	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	28	28	25	23	24	**26,5 ms**
Visszafejtés	7	6	6	4	6	**6,3 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	26	27	30	29	25	
Visszafejtés	7	5	7	8	7	
128 byte	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**

Titkosítás	24	24	26	26	25	**25,1 ms**
Visszafejtés	6	5	7	7	7	**6,3 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	21	23	28	26	28	
Visszafejtés	4	7	7	5	8	

245 byte	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	28	30	30	28	28	**25,9 ms**
Visszafejtés	7	4	5	7	6	**6 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	25	22	22	21	25	
Visszafejtés	4	9	5	7	6	

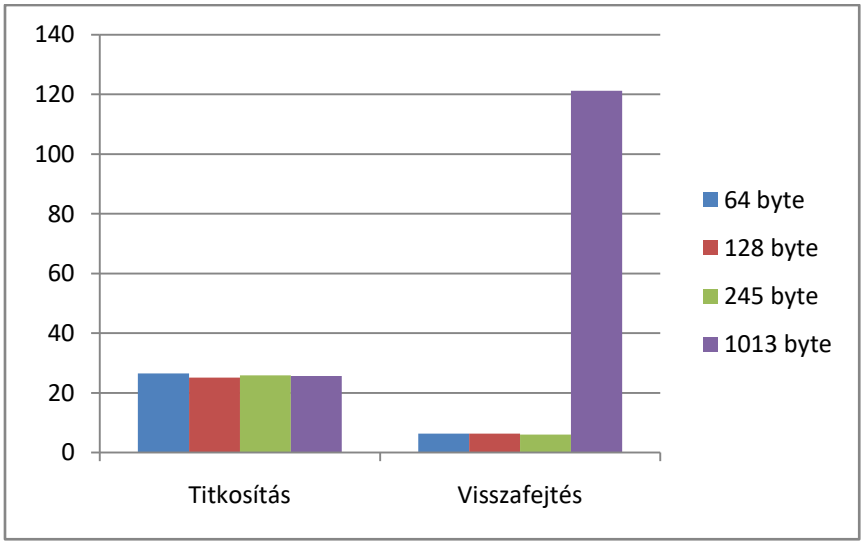
Ezután megpróbáltam nagyobb fájlokat titkosítani, így növelnem kellett a kulcs nagyságát is.

A kulcs nagysága: 8192 byte. Titkosítandó fájl nagysága: 1013 byte (a fejlécadat nagysága miatt ez lett a limit, de a kettőt összeadva egyébként 2^10-en, azaz 1024 byte). Titkosított fájl mérete: 1024 byte.

1013 byte	**1.mérés**	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás	28	21	22	31	29	**25,6 ms**
Visszafejtés	117	123	121	121	125	**121,2 ms**
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás	23	24	27	28	23	
Visszafejtés	119	122	121	119	124	

Annak ellenére, hogy ezek az értékek nem tűnnek nagynak, a számítógépemnek elég sokáig tartott minden mérés elvégzése, volt néhol 10 másodperc is, mire az eredményt megkaptam. Az említett 'System.currentTimeMillis()' metódus használatát ajánlották az interneten kód futásidejének mérésére, így nem tudom mi lehetett a probléma, de mivel már az 1 kb-os fájl titkosítása eddig tartott, nagyobb fájlmérettel nem próbálkoztam.

Függőleges tengely az eltelt idő milliszekundumban mérve.



/*
*dofinal.txt
* szinkronizációs rész (downloads-ba a message txt)

*/

----TEMPLATE-----

	1.mérés	2.mérés	3.mérés	4.mérés	5.mérés	Átlag
Titkosítás						
Visszafejtés						

	1.mérés	**2.mérés**	**3.mérés**	**4.mérés**	**5.mérés**	**Átlag**
Titkosítás						
Visszafejtés						
	6.mérés	**7.mérés**	**8.mérés**	**9.mérés**	**10.mérés**	
Titkosítás						
Visszafejtés						