ISSN 2181-3187

TURLI KRIPTOGRAFIYA ALGORITMLARINING SAMARADORLIGINI TAHLIL QILISH

Madirimova Saodatjon Madirimovna
“Ma’mun Universiteti” NTM o‘qituvchisi
Bobonazarova Munisaxon Rashidbek qizi
“Ma’mun Universiteti” NTM talabasi
Yo‘ldosheva Maxliyo Ulug‘bek qizi
“Ma’mun Universiteti” NTM talabasi

Annotatsiya: Ma'lumotlar xavfsizligi bugungi axborot texnologiyalari davrida asosiy muammo bo'lib kelgan. Bu, ayniqsa, bulutli muhitda jiddiy bo'ladi, chunki ma'lumotlar butun dunyo bo'ylab turli joylarda joylashgan. Shifrlash yechim sifatida paydo bo'ldi va turli shifrlash algoritmlari bulutdagi ma'lumotlar xavfsizligida muhim rol o'ynaydi. Shifrlash algoritmlari bulutli hisoblashda ma'lumotlar xavfsizligini ta'minlash uchun ishlatiladi. Ma'lumotlar xavfsizligini ta'minlashdan maqsad shundan iboratki, unga faqat tegishli va vakolatli foydalanuvchilar kirishi mumkin. Ushbu maqolada biz simmetrik (AES, DES, 3DES, BLOWFISH, RC4), assimetrik (RSA, DSA, Diffie-Hellman, EI-Gamal, Pailier), Hashing (MD5, MD6, SHA, SHA256) algoritmlari. Shuningdek, biz AES, DES, BLOWFISH, DES, RC4, RSA kabi beshta mashhur va keng qo‘llaniladigan shifrlash texnikasini joriy qildik va mahalliy tizimdagi turli fayl o‘lchamlari uchun shifrlash va shifrni ochish vaqtini tahlil qilish asosida ularning ishlashini solishtirdik.

Kalit so'zlar - kriptografiya algoritmlari, shifrlash, shifrni ochish. Simmetrik kalit, Asimmetrik kalit, Xeshlash algoritmlari, Kalit uzunligi

Asosiy qism: Ushbu maqola besh xil shifrlash algoritmlarini baholaydi, xususan: AES, DES, RC4, BLOWFISH, RSA, shifrlash sxemalarining ishlash ko'rsatkichlari ma'lumotlar turlari (matn yoki hujjatlar), mahalliy platformadagi kirish ma'lumotlarining turli o'lchamlari bo'yicha uzatiladi va baholanadi. turli kirish fayllari uchun o'z ishlashi. Kriptografiya "maxfiy yozish" degan ma'noni anglatadi, bu xabarlarni xavfsiz va ruxsatsiz foydalanuvchi hujumlaridan himoya qilish uchun o'zgartirish fan va san'atidir. Shifrlash - bu ochiq matnni shifrlangan matnga aylantirish jarayoni va shifrlash shifrlangan matnni yana ochiq matnga aylantiradi. Yuboruvchi shifrlash algoritmidan, qabul qiluvchi esa shifrni ochish algoritmidan foydalanadi. Shunday qilib, shifrlash va shifrni ochish xabarni xavfsiz uzatishga yordam beradi va xabarni ruxsatsiz foydalanuvchilardan himoya qiladi [1].

Quyida keltirilgan kriptografiya algoritmining uchta turi mavjud [2] [21]:
• Simmetrik kalitli kriptografiya algoritmi
• Assimetrik kalitli kriptografiya algoritmi
• Xesh kriptografiyasi

1-jadvalda AES, DES, 3DES, BLOWFISH, RC4, RSA, DSA, Diffie-Hellman, EI-Gamal, Paillier, MD5, MD6, SHA va SHA256 o'rtasidagi qiyosiy xulosa ko'rsatilgan. , Contributor, Kalit uzunligi, Davralar va Blok hajmi.

ISSN 2181-3187

1-jadval: Kriptografiya algoritmlarining xarakteristikalari

Sxema	Algoritm Turi	Himoyachi	Kalit uzunligi	Davralar	Blok hajmi
AES	Symmetric	Rijindael	128,192, 256	10 or 12 or 14	128 bits
DES	Symmetric	IBM 75	56-bits	16	64 bits
3DES	Symmetric	IBM 78	168, 112 bits	48	64 bits
BLOWFISH	Symmetric	Bruce Schneier 93	128-448 bits	-	64 bits
RC4	Symmetric	Ronald Rivest 87	40-128-bits	-	-
RSA	Asymmetric	Rivest,Shamir, Adleman 77	1024	1	Minimum 512 bits
DSA	Asymmetric	NIST 91	-	-	-
Diffie-Hellman	Asymmetric	Diffie, Hellman 76	-	-	-
EI-Gamal	Asymmetric	Elgamal 84	-	-	-
Paillier	Asymmetric	Paillier 99	-	-	-
MD5	Hashing	Rivest 91	128	-	512 bit
MD6	Hashing	Prof. Rivest 08	-	-	-
SHA	Hashing	NIST 95	160	-	-
SHA256	Hashing	-	256	-	32 bit

Barcha algoritmlarning kalit o'lchamlari bir-biridan farq qiladi. DES algoritmining kalit uzunligi 56 bit. AES algoritmining kalit hajmi 128, 192, 256 bit. Blowfish algoritmining kalit hajmi 128-448 bit. RSA algoritmining kalit hajmi 1024 bit.

Ushbu eksperimental ishda quyidagi parametrlar asosida turli xil kirish o'lchamidagi mahalliy tizimda berilgan algoritmlarning ishlashi tahlil qilinadi. Ushbu bo'limda eksperimental parametrlar, platformalar va eksperimental algoritmlarning kalit boshqaruvi tavsiflanadi.

Baholash parametrlari

1. Shifrlash vaqti: shifrlash vaqti shifrlash algoritmi oddiy matndan shifrlangan matnni yaratish uchun ketadigan vaqtni hisobga olgan.

2. Shifrni hal qilish vaqti: shifrni hal qilish algoritmi shifrlangan matndan oddiy matnni yaratish uchun ketadigan vaqtni hisobga olgan.

EXPERIMENTAL NATIJALAR VA TAHLIL

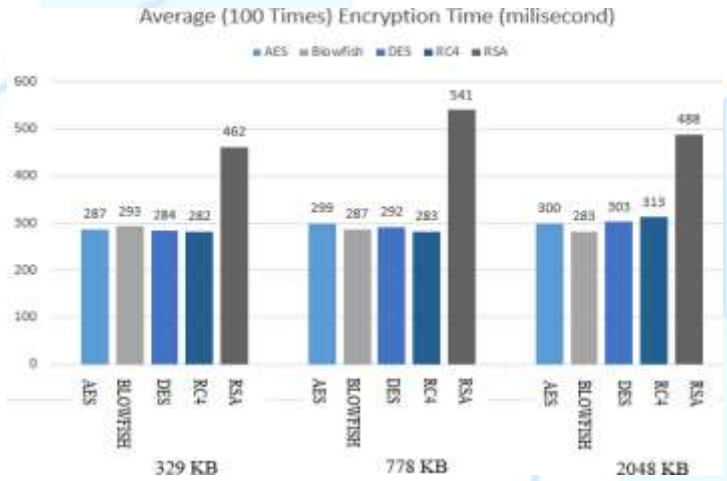
AES, BLOWFISH, DES, RC4, RSA shifrlash algoritmi bo'yicha eksperimental natija 2-jadvalda ko'rsatilgan, ularda bir nechta kirish fayl o'lchamlari amalga oshirilgan: 329 bayt, 778 bayt va 2048 bayt. Ushbu tajribada ishlatiladigan har bir algoritmning kalit o'lchami jadvalda ham ko'rsatilgan. Barcha natijalar ehtiyotkorlik bilan olinadi, yuqori aniqlikka erishish uchun umumiy bajarilish vaqtining yuz (100) namunasi olindi, so'ngra algoritmlar o'rtasida o'lchash va qiyosiy tahlil qilish, shuningdek, grafik chizish uchun o'rtacha yuzta namunalar olindi. Shifrlash va parolni hal qilish vaqti millisekundlarda hisoblanadi va kirish hajmi kilobaytlarda olinadi. Yagona tizimdagi barcha tahlil qilingan algoritmlar uchun barcha tegishli kuzatish ko'rsatkichlari va grafik ko'rsatilgan.

2-jadval: Turli algoritmlarning samaradorligini solishtirish

№	Algoritm	Kalit hajmi (bit)	Fayl hajmi (bytes)	O'rtacha (100 marta) shifrlash vaqti (millisoniya)	O'rtacha (100 marta) shifrni ochish vaqti (millisoniya)
1	AES	256	329	287	293
			778	299	304

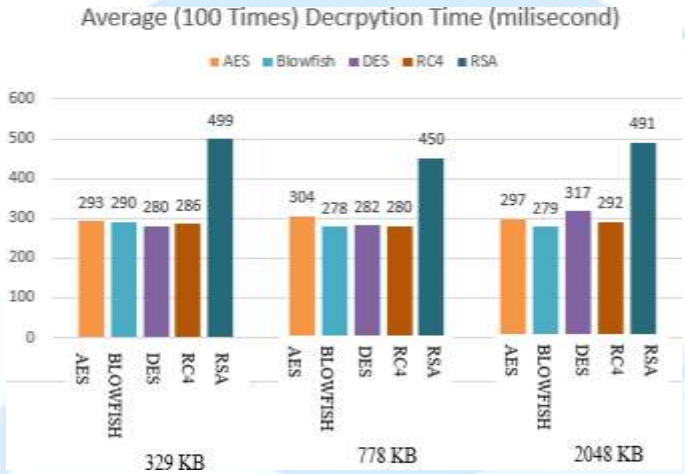
ISSN 2181-3187

			2048	300	297
2	Blow-fish	128	329	293	290
			778	287	278
			2048	283	279
3	DES	56	329	284	280
			778	292	282
			2048	303	317
4	RC4	64	329	282	286
			778	283	280
			2048	313	292
5	RSA	1024	329	462	499
			778	541	450
			2048	488	491



1-rasm: Turli algoritmlarni shifrlash vaqti (ustun asosida)

1-rasmda shifrlash vaqtini, 3-rasmda simmetrik algoritmlarning (AES, BLOFISH, DES va RC4) va assimetrik algoritmlarning (RSA) shifrlash vaqtini ham ko'rsatadi. Bundan tashqari, ikkala toifadagi barcha algoritmlar (nosimmetrik va assimetrik) DES va RSA algoritmlaridan tashqari, ish vaqti va kirish fayli hajmi o'rtasidagi mutanosiblikdan foydalanadi. DES va RSA ish vaqti kirish fayl hajmining oshishi bilan biroz o'zgaradi. 2-jadvalni tahlil qilib, RSA algoritmining shifrlash va dekodlash jarayoniga sarflagan vaqti AES, BLOWFISH, DES va RC4 algoritmlari bilan solishtirganda ancha yuqori.



2-rasm: Turli algoritmlarning shifrini ochish vaqti (ustun asosida)

XULOSA: Shifrlash algoritmi aloqa xavfsizligiga juda muhim hissa qo'shadi. Bizning tadqiqot ishimiz AES, DES va RSA algoritmlari kabi keng qo'llaniladigan shifrlash usullarining ishlashini ko'rsatdi. Amaldagi matn fayllari va eksperimental natijalar asosida AES algoritmi eng kam shifrlashni, RSA esa eng uzoq shifrlash vaqtini sarflaydi, degan qarorga keldi. Shuningdek, biz AES algoritmining shifrini ochish boshqa algoritmlarga qaraganda yaxshiroq ekanligini ko'rsatdik. Analitik natijadan shuni aytishimiz mumkinki, AES algoritmi DES va RSA algoritmlariga qaraganda ancha yaxshi. Tasvir va audio ma'lumotlarini kiritish orqali biz AES, DES va RSA kabi mavjud kriptografik algoritmlarni solishtiramiz va tahlil qilamiz va asosiy e'tibor shifrlash vaqtini va shifrni ochish vaqtini yaxshilashga qaratiladi.

Adabiyotlar

[1] Seitnazarov K.K . t.f.d dots. Madirimova S.M. Zamonaviy kriptoalgoritmlarning ishonchliligi. Kriptoalgoritmlarining xavfsizlik darajasi.
[2] S C Rachana, Dr. H S Guruprasad, “Emerging Security Issues and Challenges in Cloud Computing”, International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014, and ISSN: 2319-5967.
[3] Vineet Kumar Singh, Dr. Maitreyee Dutta “ANALYZING CRYPTOGRAPHIC ALGORITHMS FOR SECURE CLOUD NETWORK” International Journal of advanced studies in Computer Science and Engineering IJASCSE Volume 3, Issue 6, 2014.
[4] Priyanka Arora, Arun Singh, Himanshu Tyagi “ Evaluation and Comparison of Security Issues on Cloud Computing Environment” in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.
[5] Dr. Prerna Mahajan & Abhishek Sachdeva , “A Study of Encryption Algorithms AES, DES and RSA for Security ”, Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350.
[6] Randeep Kaur, Supriya Kinger “Analysis of Security Algorithms in Cloud Computing”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March 2014, ISSN 2319 – 4847.
[7] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,”Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures” IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.