МАВЖУД КРИПТОГРАФИК КУТУБХОНАЛАРНИНГ ТАҲЛИЛИ

Алланов Ориф Менглимуротович
Киберхавфсизлик ва криминалистика кафедраси мудири Фалсафа фанлари бўйича фалсафа доктори (PhD)., доц.
Абдималиков Дилмурод Ахад ўғли
Термиз давлат университети Амалий математика ва интеллектуал технологиялар факултети Компютер ва дастурий инжиниринг кафедрасининг магистранти
https://doi.org/10.5281/zenodo.11274073

Ҳозирги кунда криптографик ҳимоя ахборотнинг ишончли ҳимоялаш усуллардан бири саналиб, маълумот устида турли ўзгартиришларни (шифрлаш амаллари) амалга оширган ҳолда уни рухсат этилмаган фойдаланувчи учун тушунарсиз кўринишга олиб келади. Ушбу шифрлаш амаллари махсус алгоритмлар тўпламидан фойдаланилган ҳолда турли йўллар билан амалга оширилади.

Криптографик кутубхона – криптографик мақсадда фойдаланиш учун зарур бўлган бир қанча алгоритмларнинг тўплами бўлиб, у одатда жамланган алгоритмларни бажарадиган вазафасига кўра туркумланган ҳолда ўзида сақлайди. Ҳозирда турли дастурлар тиллари учун яратилган қатор криптографик кутубхоналар мавжуд бўлиб, уларнинг алгоритм таркиби ва амалга оширилиши турлича.

Криптографик кутубхоналарни яратишда хавфсизлик бирламчи ва муҳим талаб бўлганлиги боис, бу жараён узоқ вақт, катта харажат ва юқори малакани талаб этади. Шу боис мавжуд криптографик кутубхоналарни фойдаланишдан олдин, уларнинг хусусиятлари ҳақида ахборотга эга бўлиш талаб этилади.

Криптографик кутубхоналардаги алгоритмлар одатда қуйидагича туркумланиши мумкин:

- криптографик калитларни генерациялаш ва тақсимлаш алгоритмлари;
- блокли шифрлаш алгоритмлари;
- хэш функция алгоритмлари;
- оқимли шифрлаш алгоритмлар;
- хабарларни аутентификациялаш кодлари;
- очиқ калитли криптографик тизимлар (асосан эллиптик эгри чизиқ);
- очиқ калит криптографияси стандартлари ва ҳ.

Ушбу мақолада қуйида келтирилган кенг фойдаланилувчи криптографик кутубхоналарнинг юқоридаги омиллар бўйича таҳлили келтирилган (1-5 - жадваллар) [1, 2]:

- Botan;
- Bouncy Castle;
- cryptlib;
- Crypto++;
- Libgcrypt;
- libsodium;
- libtomcrypt;
- Nettle;
- OpenSSL;
- wolfCrypt.

1 – жадвал

Криптографик кутубхоналар хусусиятларининг қиёсий таҳлили

№	Алгоритм номи	Ишлаб чиқилган тил	Очиқ кодли	Лицензия	Мададловчи операцион тизимлар
1.	Botan	C++	+	Соддалашган BSD	Linux, FreeBSD, AIX, Windows, macOS, Android, iOS, QNX, IncludeOS
2.	Bouncy Castle	Java, C#	+	MIT лицензия	J2ME, Java Runtime Environment 1.1+, Android, Android. C# API
3.	cryptlib	C	+	Тижорий лицензия	AMX, BeOS, ChorusOS, DOS, eCOS, FreeRTOS/OpenRTOS, uItron, MVS, OS/2, Palm OS, QNX Neutrino, RTEMS, Tandem NonStop, ThreadX, uC/OS II, Unix (AIX, FreeBSD, HP-UX, Linux, macOS, Solaris, etc.), VDK, VM/CMS,

№	Алгоритм номи	Ишлаб чиқилган тил	Очиқ кодли	Лицензия	Мададловчи операцион тизимлар
					VxWorks, Win16, Win32, Win64, WinCE/PocketPC/etc, XMK
4.	Crypto++	C++	+	Очиқ лицензия	Unix (OpenBSD, Linux, macOS, etc.), Win32, Win64, Android, iOS, ARM
5.	Libgcrypt	C	+	GNU LGPL v2.1+	Барча UNIX операцион тизимлари ва Win32, Win64, WinCE
6.	libsodium	C	+	ISC лицензия	macOS, Linux, OpenBSD, NetBSD, FreeBSD, DragonflyBSD, Android, iOS, 32 ва 64-bit Windows (Visual Studio, MinGW, C++ Builder), NativeClient, QNX, JavaScript, AIX, MINIX, Solaris
7.	libtomcrypt	C	+	Очиқ	GNU/Linux, FreeBSD, macOS, Windows
8.	Nettle	C	+	GNU GPL v2+	GNU/Linux, FreeBSD, macOS, Windows
9.	OpenSSL	C	+	Apache Licence 1.0	Solaris, Linux, macOS, QNX, BSD, Windows, OpenVMS
10.	wolfCrypt	C	+	GPL v2 ёки тижорий	Win32/64, Linux, macOS, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded

№	Алгоритм номи	Ишлаб чиқилган тил	Очиқ кодли	Лицензия	Мададловчи операцион тизимлар
					Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii ва Gamecube through DevKitPro, QNX, MontaVista, NonStop, TRON/ITRON/µITRON, Micrium's µC/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP-UX

2 – жадвал

Криптографик кутубхоналарнинг қиёсий таҳлили (калитларни генерациялаш, тақсимлаш ва очиқ калитли криптографик тизимлар)

№	Кутубхона номи	Мавжуд алгоритмлар	
		Калитларни генерациялаш ва тақсимлаш	Очиқ калитли крипторафик тизимлар
1.	Botan	ECDH, DH, DSA, RSA, ElGamal, DSS	NIST, SECG, ECC Brainpool, ECDSA, Curve25519, EdDSA
2.	Bouncy Castle	ECDH, DH, DSA, RSA, ElGamal, NTRU, DSS	NIST, SECG, ECC Brainpool, ECDSA, Curve25519, GOST R 34.10
3.	cryptlib	ECDH, DH, DSA, RSA, DSS	NIST
4.	Crypto++	ECDH, DH, DSA, RSA	NIST
5.	Libgcrypt	ECDH, DH, DSA, RSA, ElGamal, DSS	NIST, SECG, ECC Brainpool, ECDSA, Curve25519, EdDSA, GOST R 34.10
6.	libsodium	DH, DSA, ElGamal, NTRU, DSS	NIST, Curve25519, EdDSA
7.	libtomcrypt	ECDH, DH, DSA, RSA	
8.	Nettle	DSA, RSA	NIST
9.	OpenSSL	ECDH, DH, DSA, RSA	NIST, SECG, ECC Brainpool,

№	Кутубхона номи	Мавжуд алгоритмлар	
		Калитларни генерациялаш ва тақсимлаш	Очиқ калитли криптографик тизимлар
			ECDSA, Curve25519
10.	wolfCrypt	ECDH, DH, DSA, RSA, NTRU, DSS	NIST, Curve25519, EdDSA

3 – жадвал

Криптографик кутубхоналарнинг қиёсий таҳлили (хэш функциялар ва хабарларни аутентификациялаш кодлари)

№	Кутубхона номи	Мавжуд алгоритмлар	
		Хэш функциялар	Хабарларни аутентификациялаш кодлари
1.	Botan	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
2.	Bouncy Castle	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
3.	cryptlib	MD5, SHA1, SHA2, SHA3, Repidm-160, Whirlpool	HMAC-MD5, HMAC-SHA1, HMAC-SHA2
4.	Crypto++	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, BLAKE2-MAC
5.	Libgcrypt	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
6.	libsodium	SHA2, Blake2	HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
7.	libtomcrypt	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
8.	Nettle	MD5, SHA1, SHA2, SHA3, Repidm-160, GOST, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES

№	Кутубхона номи	Мавжуд алгоритмлар	
		Хэш функциялар	Хабарларни аутентификациялаш кодлари
9.	OpenSSL	MD5, SHA1, SHA2, Repidm-160, Tiger, Whirlpool, GOST, Blake2, MD2, MD4,	Poly1305-AES, HMAC
10.	wolfCrypt	MD5, SHA1, SHA2, SHA3, Repidm-160, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC

4– жадвал

Криптографик кутубхоналарнинг қиёсий таҳлили (блокли шифрлаш ва шифрлаш режимлари)

№	Кутубхона номи	Мавжуд алгоритмлар	
		Блокли шифрлаш	Шифрлар режимлари
1.	Botan	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5, IDEA, GOST 28147-89	CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, AES-Wrap, Stream
2.	Bouncy Castle	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5, IDEA, GOST 28147-89	ECB, CBC, OFB, CFB, CTR, CCM, GCM, OCB, AES-Wrap, Stream
3.	cryptlib	AES-128, AES-192, AES-256, 3DES, Blowfish	ECB, CBC, CTR
4.	Crypto++	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish	ECB, CBC, CTR, CCM, GCM
5.	Libgcrypt	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5, IDEA, GOST 28147-89	ECB, CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, AES-Wrap, Stream
6.	libsodium	AES-256	CTR, GCM
7.	libtomcrypt	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5	ECB, CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, Stream
8.	Nettle	AES-128, AES-192, AES-256,	ECB, CBC, CTR, CCM, GCM

№	Кутубхона номи	Мавжуд алгоритмлар	
		Блокли шифрлаш	**Шифрлар режимлари**
		Camellia, 3DES, Blowfish	
9.	OpenSSL	AES-128, AES-192, AES-256, Camellia, 3DES, CAST5, IDEA	CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, AES-Wrap, Stream
10.	wolfCrypt	AES-128, AES-192, AES-256, Camellia, 3DES, IDEA	ECB, CBC, CTR, CCM, GCM

5– жадвал

Криптографик кутубхоналарнинг қиёсий таҳлили (очиқ калит стандартлари ва оқимли шифрлаш алгоритмлари)

№	Кутубхона номи	Мавжуд алгоритмлар	
		Очиқ калит стандартлари	**Оқимли шифрлаш алгоритмлари**
1.	Botan	PKCS#1, PKCS#5, PKCS#8, IEEE P1363, ASN.1	RC4, Salsa20, ChaCha
2.	Bouncy Castle	PKCS#1, PKCS#5, PKCS#8, PKCS#12, IEEE P1363, ASN.1	RC4, HC-256, Salsa20, ChaCha, Grain, VMPC, ISAAC
3.	cryptlib	PKCS#1, PKCS#5, PKCS#8, PKCS#12, ASN.1	RC4
4.	Crypto++	PKCS#1, PKCS#5, IEEE P1363, ASN.1	RC4, Salsa20, SEAL, Panama, WAKE
5.	Libgcrypt	PKCS#1, PKCS#5, PKCS#8, PKCS#12, IEEE P1363, ASN.1	RC4, Salsa20, ChaCha
6.	libsodium		Salsa20, ChaCha
7.	libtomcrypt	PKCS#1, PKCS#5, PKCS#8, ASN.1	RC4, ChaCha
8.	Nettle	PKCS#1, PKCS#5	RC4, Salsa20, ChaCha
9.	OpenSSL	PKCS#7, PKCS#12, ASN.1	RC4, ChaCha
10.	wolfCrypt	PKCS#1, PKCS#5, PKCS#8, PKCS#12, ASN.1	RC4, HC-256, Rabbit, Salsa20, ChaCha

Олинган таҳлил натижалари мос дастурлаш тилига қараб кутубхонани танлашда, криптографик алгоритмлардан хавфсиз фойдаланишда, алгоритмларнинг тезлик бўйича таққослашда катта самара беради. Ушбу кутубхоналардан фойдаланиш код қаторини

камайтиришга, хавфсиз кодни яратишга ва сарфланадиган вақт ҳажмини камайишига сабабчи бўлади.

Юқорида келтирилган таҳлил натижаларидан шуни билиш мумкинки, аксарият кутубхоналар халқаро алгоритмлар ёки АҚШ стандартлари ва камдан – кам ҳолда Россия давлат стандартларини ўз ичига олган. Шуни ҳисобга олган ҳолда, миллий стандартларни ўз ичига олган криптографик кутубхонани яратиш долзарбдир. Шунинг учун ушбу криптографик кутубхонани яратиш кейинги тадқиқот ишининг мақсади қилиб олинди.

Фойдаланилган адабиётлар:

1. Locke G., Gallagher P. Fips pub 186-3: Digital signature standard (dss) //Federal Information Processing Standards Publication. – 2009. – Т. 3. – С. 186-3.
2. https://dotnet.microsoft.com/learn/dotnet/what-is-dotnet
3. https://www.oracle.com/java/technologies/java-se.html
4. https://en.wikipedia.org/wiki/Comparison_of_cryptography_libraries