МАВЖУД КРИПТОГРАФИК КУТУБХОНАЛАРНИНГ ТАҲЛИЛИ

Алланов Ориф Менглимуротович
Киберхавфсизлик ва криминалистика кафедраси мудири, Техника 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.11450064

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
	Botan	C++	+	Соддалашган BSD	Linux, FreeBSD, AIX, Windows, macOS, Android, iOS, QNX, IncludeOS
	Bouncy Castle	Java, C#	+	MIT лицензия	J2ME, Java Runtime Environment 1.1+, Android, Android. C# API
	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,

№	Алгоритм номи	Ишлаб чиқилган тил	Очиқ кодли	Лицензия	Мададловчи операцион тизимлар
					Unix (AIX, FreeBSD, HP-UX, Linux, macOS, Solaris, etc.), VDK, VM/CMS, VxWorks, Win16, Win32, Win64, WinCE/PocketPC/etc, XMK
	Crypto++	C++	+	Очиқ лицензия	Unix (OpenBSD, Linux, macOS, etc.), Win32, Win64, Android, iOS, ARM
	Libgcrypt	C	+	GNU LGPL v2.1+	Барча UNIX операцион тизимлари ва Win32, Win64, WinCE
	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
	libtomcrypt	C	+	Очиқ	GNU/Linux, FreeBSD, macOS, Windows
	Nettle	C	+	GNU GPL	GNU/Linux,

№	Алгоритм номи	Ишлаб чиқилган тил	Очиқ кодли	Лицензия	Мададловчи операцион тизимлар
				v2+	FreeBSD, macOS, Windows
	OpenSSL	C	+	Apache Licence 1.0	Solaris, Linux, macOS, QNX, BSD, Windows, OpenVMS
	wolfCrypt	C	+	GPL v2 ёки тижорий	Win32/64, Linux, macOS, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded 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
	Botan	ECDH, DH, DSA, RSA,	NIST, SECG, ECC

№	Кутубхона номи	Мавжуд алгоритмлар	
		Калитларни генерациялаш ва тақсимлаш	Очиқ калитли криптографик тизимлар
		ElGamal, DSS	Brainpool, ECDSA, Curve25519, EdDSA
	Bouncy Castle	ECDH, DH, DSA, RSA, ElGamal, NTRU, DSS	NIST, SECG, ECC Brainpool, ECDSA, Curve25519, GOST R 34.10
	cryptlib	ECDH, DH, DSA, RSA, DSS	NIST
	Crypto++	ECDH, DH, DSA, RSA	NIST
	Libgcrypt	ECDH, DH, DSA, RSA, ElGamal, DSS	NIST, SECG, ECC Brainpool, ECDSA, Curve25519, EdDSA, GOST R 34.10
	libsodium	DH, DSA, ElGamal, NTRU, DSS	NIST, Curve25519, EdDSA
	libtomcrypt	ECDH, DH, DSA, RSA	
	Nettle	DSA, RSA	NIST
	OpenSSL	ECDH, DH, DSA, RSA	NIST, SECG, ECC Brainpool, ECDSA, Curve25519
	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
	Botan	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC

№	Кутубхона номи	Мавжуд алгоритмлар	
		Хэш функциялар	Хабарларни аутентификациялаш кодлари
	Bouncy Castle	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
	cryptlib	MD5, SHA1, SHA2, SHA3, Repidm-160, Whirlpool	HMAC-MD5, HMAC-SHA1, HMAC-SHA2
	Crypto++	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, BLAKE2-MAC
	Libgcrypt	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
	libsodium	SHA2, Blake2	HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
	libtomcrypt	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
	Nettle	MD5, SHA1, SHA2, SHA3, Repidm-160, GOST, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES
	OpenSSL	MD5, SHA1, SHA2, Repidm-160, Tiger, Whirlpool, GOST, Blake2, MD2, MD4,	Poly1305-AES, HMAC
	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
	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
	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
	cryptlib	AES-128, AES-192, AES-256, 3DES, Blowfish	ECB, CBC, CTR
	Crypto++	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish	ECB, CBC, CTR, CCM, GCM
	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
	libsodium	AES-256	CTR, GCM
	libtomcrypt	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5	ECB, CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, Stream
	Nettle	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish	ECB, CBC, CTR, CCM, GCM
	OpenSSL	AES-128, AES-192, AES-256, Camellia, 3DES, CAST5, IDEA	CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, AES-Wrap, Stream
	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
	Botan	PKCS#1, PKCS#5, PKCS#8, IEEE P1363, ASN.1	RC4, Salsa20, ChaCha
	Bouncy Castle	PKCS#1, PKCS#5, PKCS#8, PKCS#12, IEEE P1363, ASN.1	RC4, HC-256, Salsa20, ChaCha, Grain, VMPC, ISAAC
	cryptlib	PKCS#1, PKCS#5, PKCS#8, PKCS#12, ASN.1	RC4
	Crypto++	PKCS#1, PKCS#5, IEEE P1363, ASN.1	RC4, Salsa20, SEAL, Panama, WAKE
	Libgcrypt	PKCS#1, PKCS#5, PKCS#8, PKCS#12, IEEE P1363, ASN.1	RC4, Salsa20, ChaCha
	libsodium		Salsa20, ChaCha
	libtomcrypt	PKCS#1, PKCS#5, PKCS#8, ASN.1	RC4, ChaCha
	Nettle	PKCS#1, PKCS#5	RC4, Salsa20, ChaCha
	OpenSSL	PKCS#7, PKCS#12, ASN.1	RC4, ChaCha
	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