Yana E. Kolegova-Delcheva,

CRYPTOGRAPHY - A PART OF CYBER SECURITY IN THE ARMED FORCES

Yana E. Kolegova-Delcheva

***Abstract**: In the following report, we examined the topic cybersecurity and cryptography as part of it. The concept of cryptography is being defined along with a brief description of the main terms and objectives. A brief classification of the different cryptography types according to the types of cryptography keys used is also present. The need of using cryptography in the armed forces as one of the main means of achieving cybersecurity has been analysed too.*

***Keywords**: cybersecurity, cryptography, armed forces, cryptosystem, key*

КРИПТОГРАФИЯТА - ЧАСТ ОТ КИБЕРСИГУРНОСТТА ВЪВ ВЪОРЪЖЕНИТЕ СИЛИ

Яна Е. Колегова-Делчева

kolegova@abv.bg

1. Увод

Още от древността различните племена са водили битки помежду си за завладяване на територии. С развитието на човечеството, със създаването на националната държава, светът навлиза в една нова фаза от своето съществуване. Пред лидерите на страните се появява един нов спектър от задачи и приоритети, които трябва да изпълнят, за да съумеят да запазят и съхранят националната си идентичност и просперитет. Една такава задача е опазване на сигурността и гарантирането на спокойно съществуване на гражданите в периметъра на националните граници. Светът преминава през две катастрофални войни – Първата и Втората световна война, а страхът от избухването на трета взема превес и държавите осъзнават, че осигуряването на мир и стабилност ще доведат до пълноценно развитие на човечеството. След тези войни вече започва да се говори не само за национална, но и за глобална политика на сигурност. Бързото развитие на технологиите, компютрите, появата на интернет и цифровизацията на системите служат както в помощ на правителствените структури, но също така крият своите опасности за националната и световната сигурност. Осигуряването на киберсигурност се е превърнало в неизменна част от политиката на всяка страна. Киберсигурността се свързва с осигуряването на «*защита на свързаните с интернет системи, включително хардуер, софтуер и данни, от кибератаки*» [12] .Киберсигурността представлява приемането на защитни механизми и мерки срещу неоторизирания достъп до центрове за данни и други компютърни системи. Изграждането на ефективни и адекватни мерки за киберзащита е сравнително нова област на загриженост от страна на военните и правителствените организации. Ниската цена на компютърните устройства и компоненти, както и свободното разпространение на технологиите са предпоставка за превръщането на много хора в потенциални

„контрабандисти" на информация. Пазарът за откраднатa информация е доста богат и се превръща дейността по търговията с информация в процъфтяващ и печеливш бизнес по целия свят. [7]

2. Криптография

Информационните системи на Министерство на отбраната и въоръжените сили, както и всички специализирани организации имат нужда от особено мощна киберзащита, защото загубата на класифицирана информация или данни не е опция в отбранителния сектор и военните организации. Голяма част от приложенията и класифицираната комуникация са силно защитени чрез жизненото и необходимо криптиране[13].

2.1. Дефиниция

Криптографията е свързана с процеса на преобразуване на текстово съобщение от разбираем текст в неразбираем и обратното. Тя представлява метод „*за съхраняване и предаване на данни в определена форма, така че само тези, за които е предназначен, могат да го четат и обработват* [11] ". В чл. 84, Раздел 4 от Закон за защита на класифицираната информация /ЗЗКИ/ криптографската сигурност е дефинирана, като „*...система от криптографски методи и средства, които се прилагат с цел защита на класифицираната информация от нерегламентиран достъп при нейното създаване, обработка, съхраняване и пренасяне.*[1]" Именно чрез криптографията се защитават голяма част от мрежите и системите, защото тя служи не само за защита на данните от кражба или промяна, *„но може да се използва и за удостоверяване на потребителя* [1]". В съвременния свят криптографията представлява пресечна точка между математическата теория и практиката на компютърните науки.

2.2. Основни понятия

Няколко са основните понятия свързани с криптографията, а именно:

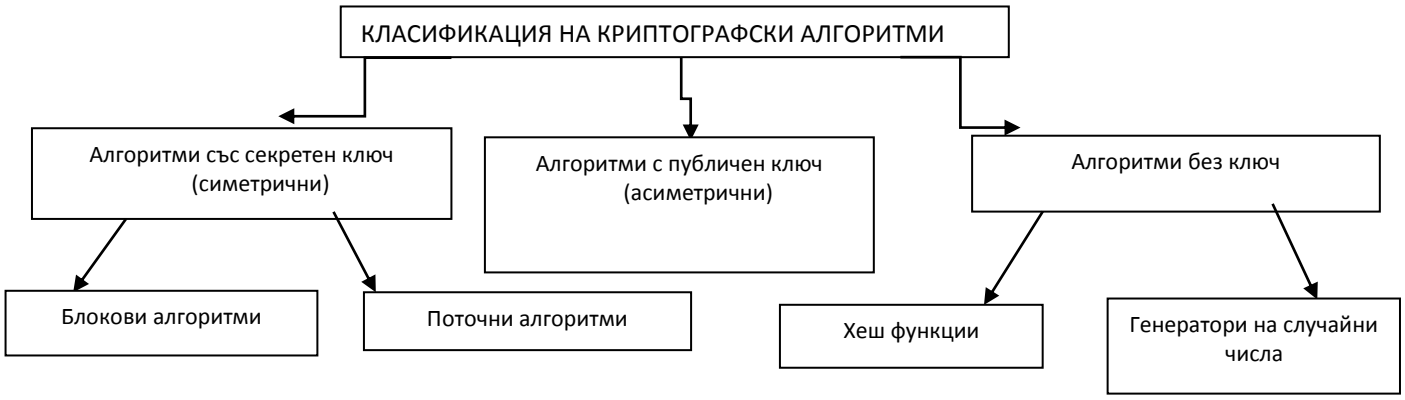
- Криптиране (encryption) – преобразуване на текстовото съобщение, по такъв начин, че то да остане неразгадаемо, за всеки, за който не е предназначено.
- Декриптиране (decryption) – обратната операция. Декодиране на съобщението в явен текст.
- Криптографски алгоритъм (cryptographicalgorithm) – преобразуването на данни в неразбираеми последователности от символи и тяхното правилно обратно възстановяване.
- Явен текст (plaintext) – първоначалния, оригинален текст, преди той да бъде шифриран с криптографски алгоритъм.
- Криптиран текст (ciphertext) – получената символна поредица, след криптирането на явния текст.
- Криптографски протокол (cryptographicprotocol) - правилото за обмен на данни и използване на криптографския алгоритъм.
- Криптосистема (cryptosystem) - съвкупността от криптографския алгоритъм и критрографския протокол.
- Криптографски ключ (key) - множество от числа или символи, което се използва за криптиране или декриптириране на съобщенията . Ключът бива два вида: ако е запазен в тайна (secretkey) и ако е известен, се нарича публичен ключ (publickey).
- Криптоанализът (cryptanalysis) е наука, занимаваща се с разработката на методи и средства за разкриване (на тайната) на криптографските системи и за оценка на тяхната сигурност.
- Криптология (cryptology) е обобщена дисциплина, включваща криптографията и криптоанализа [14].

2.3. Цели

Целта на криптографската система е да се предотврати нерегламентирано проникване в системите и неразрешеното извличане на информация и данни, т.е. да се осигури нейната **конфиденциалност**. Друга основна цел на криптографията е да се осигури **целостта** на информацията, т.е. да се предотврати възможността данните да бъдат променени или манипулирани по някакъв начин. **Истинността** определя дали дадено лице в интернет е реално, като се проверява не само самоличността на подателя на съобщението, но и на получателя. Друга основна цел е осигурява-

нето на **достъпност** на информацията, т.е. да се гарантира, че кодираните данни ще попаднат в правилните ръце.

2.4. Класификация на криптографски алгоритми



Таб. 1 – Класификация на криптографски алгоритми, спрямо използването на ключове - http://netseclab.tu-sofia.bg/vbook/Glava10.pdf, стр.228 [2]

3. Криптографията и въоръжените сили

Когато говорим за военните криптографски системи, трябва да се имат в предвид редица практически измерения. Тя трябва да представлява единна универсална система, предназначена за практична употреба от най-високо до най-ниско йерархично равнище. Използването на криптографията за защита на военната информация има своите немалко предимства. На първо място, криптографията представлява надежден механизъм за защита на база данни, независимо от броя на съобщенията, които се изпращат. От друга страна тя работи при всички климатични условия и не изисква специално обучение на потребителите. Разбира се не всяка система отговаря на тези условия. Изборът на криптографска система за военна употреба трябва да се свързва с осигуряване на сигурността, запазване на целостта, достоверността и поверителността на информацията. Същевременно, защитавайки информацията от нерегламентиран достъп, системата трябва да осигурява бърза и надеждна комуникация и да обслужва нуждите на всички участници в нея. Ако се използва криптографска система, която изисква един час за криптиране на данните, която е толерантна към направата на грешки при използването ѝ, ако не може да се използва при определени климатични условия, ако поддържа нисък обем от съобщения и изисква скъпо и сложно оборудване, то тя би била напълно неподходяща за използването за военни цели. Разбира се нито една система не отговаря на абсолютно всички изисквания за сигурност, надеждност, гъвкавост и цена. Затова при изборът на криптографска система за опазване на военна информация трябва да се търси баланс между тези практически изисквания и да се избере системата, която има най-малко уязвимости, която би могла да осигури сигурността при обмена на информацията.

Когато говорим за криптографските системи, трябва да отчетем и фактът, че са податливи на уязвимости. Има няколко фактора, които могат да спомогнат за осъществяването на криптоаналитична атака. Един от най-важните фактори е криптографската стабилност, т.е. колкото по-малко повтаряне на ключовете и ограничени модели за използване има, толкова по-голяма е устойчивостта на системата. Колкото по-дълго време се използват ключовете без промяна, толкова по-голяма е вероятността да се открие уязвимост в системата и да се проникне в нея. Една от най-важните роли за сигурността в системата играят системните потребители, за които има написания ясни правила за употреба. Смесването на явен текст с кодиран в едно съобщение, направата на неоторизирани промени или опростяване в системата, обсъждането на съдържанието на крипти-

раните съобщения и на системата и нейните ключове, могат да доведат до осъществяването на успешна кибератака [15].

4. Изводи

4.1. Сигурността на държавите отдавна е преминала отвъд националните граници и се е превърнала в транснационална, което налага приемането на общи политика за сигурност и сътрудничество в сферата на отбраната, комуникацията, транспорта, енергетиката и др.

4.2. Криптографията е едно от надеждните средства за осъществяването на адекватна, ефективна и ефикасна политика за киберсигурност.

4.3. Използването на уязвимостите в мрежите на критичните инфраструктури, налага използването на криптографията, като алгоритъм за защита на поверителността, целостта на данните.

4.4. Когато се говори за криптографска сигурност трябва специалистите по киберзащита да са наясно с определените дефиниции, понятия, цели и типове криптография.

4.5. Необходимо е да се инвестират повече средства в хора, технологии, научноизследователска дейност, за да могат военните да проучат съвременните заплахи в киберпространството и да открият възможните начини да защитят своите мрежи от неправомерни действия.

5. Заключение

Съвременното бойно поле отдавна е излезнало извън рамките на традиционното и вече започват да се появяват все повече неконвенционални оръжия. Бойният терен се прехвърли в киберпространството, което поражда нуждата от вземането на специални механизми за киберсигурност във всички сфери от обществения и личния живот. Компютърните системи са все по-чувствителни и уязвими, а процеси като глобализацията, разпространението и производството на компютърна техника, не достатъчната подготовка на хората за работа със системите, многобройните заплахи от нападения или манипулации застрашават работата на модерните информационни системи. Киберсигурността включва защита на военните мрежи срещу киберзаплахи. Киберпространството е мрежа от мрежи, която включва безброй компютри по целия свят, поради което нито една държава или организация не може едностранно да поддържа ефективна киберсигурност [9]. Именно в такъв тип мрежа, която се използва от голям брой потребители, криптографията често е от съществено значение за защитата, както на съхранените, така и на предаваните данни. Всяка една мрежа изисква използването на определен крипрографски алгоритъм, който да отговаря на нуждите на системата, за да гарантира сигурността. Колкото и да е сигурна, дори криптографската система има своите уязвимости и слаби места и основна задача на експертите по киберсигурността е да откриват тези „слаби места" и да създават алгоритми, с които системите да останат неприкосновени.

References

1. **Закон** за защита на класифицираната информация. https://www.lex.bg/laws/ldoc/2135448577

2. **Ненова** М. Въведение в приложната криптография. http://netseclab.tu-sofia.bg/nsk/lectures_nsk/L6.pdf

3. **Трифонов** Р. Системи за сигурност. Подписване на електронен документ с последваща валидация. http://archive.uktc-bg.com/SISTI_SIGURNOST/UPR-3_06-14.pdf

4. **Al-Vahed Ahmed, Haddad Sahhavi** (2011). An overview of modern cryptography. https://pdfs.semanticscholar.org/46d6/fee601a4f89b448deff8af7fce9c52d68501.pdf

5. **Diffie** Whitfield, Martin E. Hellman. Multiuser cryptographic techniques. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.892.6389&rep=rep1&type=pdf

6. **Koch** Robert, Mario Golling (2016). Weapons Systems and Cyber Security – A Challenging Union. https://ccdcoe.org/uploads/2018/10/Art-12-Weapons-Systems-and-Cyber-Security-A-Challenging-Union.pdf

7. Mulazzani Fabio**,** Lt.Col. Salvatore A. SARCIA (2011). Cyber Security on Military Deployed Networks. A Case Study on Real Information Leakage.
https://ccdcoe.org/uploads/2018/10/CyberSecurityOnMilitaryDeployedNetworks-Mulazzani-Sarcia.pdf

8. Rashid Awais, George Danezis, Howard Chivers, Emil Lupu and Andrew Martin (November 10, 2017) – CYBOK. Scope for the Cyber Security Body of Knowledge.
https://www.cybok.org/media/downloads/CyBOKScopeV2.pdf

9. Seng Alan Ho Wei. Cyber Attacks and the Roles the Military Can Play to Support the National Cyber Security Efforts -
https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/v42n3%204%20Cyber%20Attacks%20and%20the%20Roles%20the%20Military%20can%20play.pdf

10. **Snyder**, Don, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, Michael H. Powell. Cybersecurity of Air Force Weapon Systems. Ensuring Cyber Mission Assurance Throughout a System's Life Cycle.
https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9800/RB9835/RAND_RB9835.pdf

11. https://economictimes.indiatimes.com/definition/cryptography

12. https://searchsecurity.techtarget.com/definition/cybersecurity

13. https://www.stormshield.com/solutions/by-industry/defense-and-military-organizations/

14. http://netseclab.tu-sofia.bg/vbook/Glava10.pdf

15. http://www.umich.edu/~umich/fm-34-40-2/ch2.pdf