Тема 6

Криптография

Увод

- В дигиталната ера информацията е най-ценният **актив** на една организация, а е особено важна и за отделния човек.
- ИС не се свежда само до това да се опитваме да защитим файловете, инф. системи, корпоративната мрежа или да обучаваме персонала.
- Каквито и мерки да сме предприели 100% сигурност няма, затова се налага да прилагаме моделът на слоеве (**layered security model**), за да сме максимално защитени.
- Когато се налага да обработваме особено **чувствителна информация и лични данни** се препоръчва задължително да се прилага и един допълнителен контрол за сигурност.
- Това е **криптирането**.
- То цели информацията (съществуването или смисълът ѝ)да бъде запазена в **тайна**.

. . .

- За да запазим една информация в **тайна** е необходимо:

1)да я скрием - спомнете си т.нар. невидимо мастило;

2)да я замаскираме – напр. в текст може да се вмъкнат думи, които да формират съобщение, но известно само на човек, който знае къде да търси тези думи;

3)да я преобразим – типичен пример е: на буква да съпоставим цифра или число или т.нар. пиктограми от древността.

- Тези начини се използват от древността та до днес.
- В древността, когато малцина са могли да четат и пишат (вкл. на чужд език) е било достатъчно да **напишеш** информацията и да я прибереш на тайно място.
- В днешната практика се използва помощта на **криптографията** за същите цели.

1)

2)

Аз съм 30 годишен мъж от Пловдив.
Завършил съм Информатика във ФМИ и обичам да програмирам.
Търся работа като програмист на Java във фирма в София.
Ключ (1-1, 2-7, 3-6)

3)

Какво е криптография? Някои дефиниции

- Криптографията (от гръцките думи κρυπτός, криптос - "скрит", и γράφω, графо - "пиша"), е наука, която се занимава с теорията и практиката на скриване на информация.
- Криптографията е изучаването на това как да се променят съобщенията ни, така че някой, който ги прихване да не може да ги прочете без подходящия алгоритъм или ключ.
- Обработка на данни до неразбираема форма, която е обратима, без обаче данните да се загубят. Обикновено това става в цифров вид.

Какво е криптография? (прод.)

- Днес криптографията се счита за клон едновременно на математиката и информатиката и е тясно свързана с теорията на информацията, информационната сигурност и техническите науки.
- Мрежовата сигурност, компресирането, интернет достъпът, заключването на персоналните компютри и смартфоните и криптирането на секретни съобщения са немислими без тази наука.
- Основната **функция** на криптографията си остава скриване на значението на съобщенията, както и в някои случаи скриване на самите съобщения.

Основни понятия

- **Открит** (оригинален) текст — данни (не задължително текстови), предавани без използване на криптография.
- **Шифрован** текст — данни, получени след използване на криптосистема с указан ключ.
- **Криптосистема** (криптиращ алгоритъм) — множество обратими преобразувания на откритият текст в шифрован.
- **Ключ** — параметър на шифъра, определящ избора на конкретно преобразуване на даденият текст. В съвременните шифри алгоритъма на шифриране е известен и криптографичната устойчивост на шифъра изцяло се определя от секретността на ключа.

Основни понятия (прод.)

- **Криптоанализ** — наука, изучаваща математическите методи за нарушаване на конфиденциалността и цялостността на информацията. С други думи методи за разгадаване на оригиналния текст без да е известен ключът.
- **Шифриране** (криптиране) — процес на прилагане на криптографско преобразуване на открит текст на основата на алгоритъм и ключ, в резултат на което се създава шифрован текст.
- **Дешифриране** (декриптиране) — процес на прилагане на криптографско преобразуване на шифриран текст в открит.
- **Криптографска устойчивост** — способността на криптографския алгоритъм да противостои на криптоанализ.

В миналото

- Ранните начини за криптиране използвали транспониране. То представлява просто пренареждане реда на буквите в съобщението.
- Разбира се, това пренареждане трябва да следва някакъв ред/последователност, или получателят не би бил в състояние да възстанови съобщението.
- Спартанците са едни от първите използвали криптиране. Използва се пръчка с определен диаметър, а съобщението се пише на навита на пръчката лента от кожа странично.

Когато лентата се размотае съобщението е не четимо. Получателят знае диаметъра на пръчката и може да прочете съобщението.

. . .

- Други ранни опити за криптиране използват замяна.
- Алгоритъм за замяна просто замества всеки символ в съобщението с друг символ. Шифърът на Цезар е пример за алгоритъм за замяна. Всеки символ се заменя с друг стоящ на 3 позиции след него в азбуката. Такъв шифър е използвал Юлий Цезар за комуникация с генералите си.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Предварително се уговаря от къде да започне замяната и буквите от съответната азбука могата да се заменят. В таблицата А ще се замени с D.

“The administrator password is password” - оригинал

“Wkh dgplqlvwudwru sdvvzrug lv sdvvzrug” - криптирано

. . .

- **Polybius Cipher** всяка буква може да бъде заменена от две цифри, например A е 11

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Пример:

Открит текст: This is a secret message

Шифрован текст: 44232443 2443 11 431513421544 32154343112215

- **Multi-Alphabet Substitution** заместване на буквите

С различна дължина. Например ако имаме следната схема/шифър (+1, +2 и +3), първата буква от оригиналното съобщение ще се замести от +1 буква от азбуката, втората от +2 и т.н. Вижте пример на: http://www.counton.org/explorer/codebreaking/vigenere-cipher.php

Transposition Ciphers

- **Rail Fence cipher**
- Оригинално съобщение: Give each soldier a meal

g		v		e		c		s		l		i		r		m		a	
	i		e		a		h		o		d		e		a		e		l

- Криптирано съобщение: GVECSLIRMAIEAHODEAEL
- Може да се използват и няколко реда за подреждане на символите.

- Други методи използващи транспониране. Може да се използват и транспониране/преместване по колони и др. Route cipher, Columnar transposition, Double transposition, Grilles , …

. . .

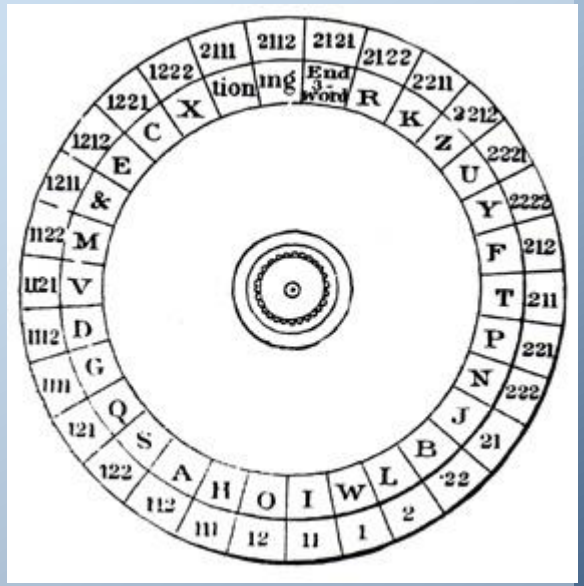
- Съвременните шифри(началото на 20 в.) са сложни алгоритми за криптиране, които работят с високоскоростни компютри, но произхода им е прости физически устройства и шифри използвани в близкото минало.
- Един пример за такова устройство е шифър диска. Използван и от Томас Джеферсън.
- **Енигма Машината**
- Днешните шифри могат също да използват

старите техники под една или друга форма.

- **Book Cipher**

Популярен от филмите за шпиони. Използва се

книга, в която се търси страница, ред и дума на реда.



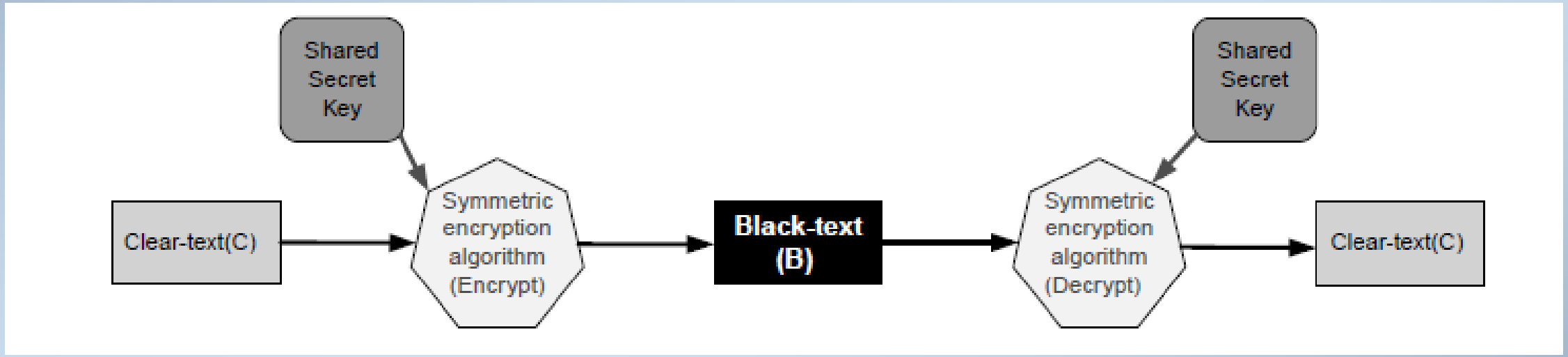
Криптография със симетричен ключ

- При този криптографски метод, двете страни обменящи информация разполагат с предварително придобит, еднакъв ключ(нар. секретен). Подателят обработва информацията, използвайки ключа по определен алгоритъм, данните се предават по комуникационния канал и след това се възстановяват при получателя.
- Ключът се използва, както за **криптиране**, така и за **декриптиране**.
- Такива ключове се наричат **споделени** секретни.
- Този метод позволява много бързо криптиране и декриптиране, затова може да се използва успешно при „бавни“ компютри.
- Недостатък на този метод е необходимостта от предварителен **обмен** (ключът да достигне получателя), както и последващото съхранение на ключовете, така че те да не бъдат откраднати.
- Пример - SSL/TSL използва този метод, когато вече е установена сигурна връзка между клиента и сървъра.

Криптография със симетричен ключ (прод.)

- Симетричният ключ, който използват и изпращачът и получателят може да бъде парола, произволен низ от символи или цифри генерирани от т.нар. secure random number generator (RNG) или pseudo-random number generator (PRNG)
- Съществуват два типа алгоритми за симетрично криптиране:
- **Блокови алгоритми.** Определен брой битове се криптират в блокове с определен ключ. Докато данните се криптират, системата съхранява данните в паметта си, докато чака завършени блокове. AES, DES, IDEA, Blowfish, RC5 и RC6
- **Поточни алгоритми.** Данните се криптират като потоци (streams) вместо да бъдат оставяни за период в системната памет. RC4

Криптография със симетричен ключ (схема)



Криптография със симетричен ключ (прод.)

Предимства на симетричното криптиране:

- Голяма скорост на шифриране/дешифриране, което му дава възможност да работи с големи масиви данни.
- Лесни за реализация;

Недостатъци на симетричното криптиране:

- Секретният ключ е само един и всяка от страните, работещи с него, може да го компрометира. Това налага честа смяна на използваните ключове;
- В мрежа с голям брой участници е необходимо поддържане, разпределение и осигуряване секретността на голям брой ключове.

Алгоритми, използвани в симетричното криптиране

DES (Data Encryption Standard)

Алгоритъмът е създаден от IBM и през 1977 г. е одобрен като стандарт за САЩ. Скоро DES се превръща в световен стандарт. Трансформира блок данни с дължина 64 бита и използва ключ с дължина 56 бита. Като стандарт е описан в документите FIPS81, ISO 8731-1, ANSI X3.92 и ANSI X3.106. Използван е за граждански цели. Заменен е със стандарта AES.

3-DES (Triple Data Encryption Standard)

Алгоритъмът представлява развитие на DES, като използва трикратно последователно шифриране чрез DES и 168-битов ключ. 3DES и модификациите му са описани в документите ISO 8372 и ANSI X3.52. Притежава висока степен на надеждност.

IDEA (International Encryption Algorithm)

Алгоритъмът е базиран на структурите на Фейстел и се състои от 8 идентични цикъла, следвани от изходна трансформация. Шифрира 64-битов блок от изходни данни в 64-битов блок шифрирани данни, като използва 128-битов ключ. При всяка итерация се използват шест 16-битови подключа. IDEA е 3 пъти по-бърз от 3-DES и е по-сигурен. Търговското му използване е свързано с заплащане на лицензионна такса.

AES (Advanced Encryption Standard)

Блоков алгоритъм, който работи с ключове с дължина 128, 192 и 256 бита. Явява се наследник на DES. Базиран е на Rijndeal Block Chiper с автори Joane Daemen иVincent Rijndael - белгийски криптографи. Това е най-използваният стандарт за симетричен алгоритъм за криптиране.

Криптография с асиметричен/публичен ключ

- Криптографията с публичен ключ (асиметричен метод) е особено важна за осигуряване на сигурното предаване на данни в Интернет.
- За разлика от метода със симетрични ключове, тук ключовете са два и се генерират едновременно по определен алгоритъм, като всеки желаещ да обменя криптирани данни, трябва да има своя собствена уникална двойка от публичен и частен ключове:

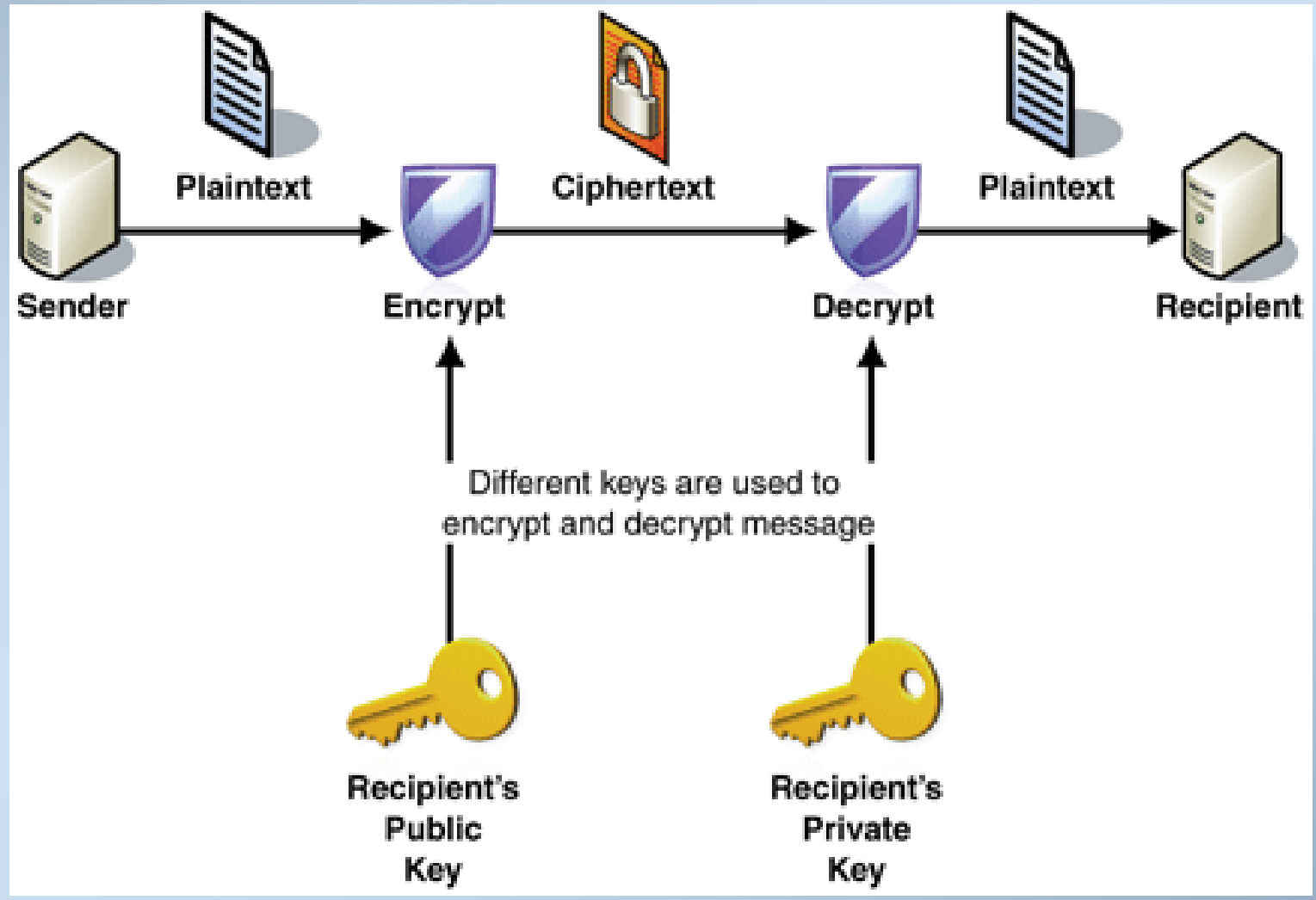
➢ **публичен ключ** - използва се за криптиране на данните и е общодостъпен за всеки, който иска да изпрати информация на притежателя му. Той не може да декриптира данните. Публичният ключ обикновено е свързан с идентичност от/чрез сертифициращ орган(Certificate Authority)

➢ **частен ключ** - достъпен е само за притежателя си. Използва се за декриптиране на криптирани с публичния ключ данни.

Криптография с публичен ключ (прод.)

- Голямото значение на криптографията с публичен ключ произтича от липсата на необходимост от предварително разпределяне или обмяна на ключове между комуникиращите страни.
- Това прави възможно предлагането на редица онлайн услуги, като електронни разплащания, сигурен обмен на данни и др.
- Поради по-голямата изчислителна интензивност, необходима за реализиране на алгоритмите за криптиране с публичен ключ, понякога методът се прилага за кратък комуникационен обмен, при който двете страни обменят ключове за продължаване на по-нататъшната комуникация чрез криптиране със симетрични ключове.
- Пример - SSL/TSL използва този метод, за установяване на сигурна връзка между клиента и сървъра. След това установяване се използва симетрично криптиране със секретен ключ.

Asymmetric Cryptography (схема, Microsoft, 2005)



Криптография с публичен ключ

Предимства на системите с асиметрично криптиране:

- Двойката ключове (частен и публичен) могат да се използват за дълъг период от време - до няколко години;
- За разлика от симетричните, в мрежа с N участници броят на поддържаните ключове е равен на броя на участниците;
- Позволяват изграждане на надеждна и ефективна схема за електронно подписване и верифициране на данни.

Недостатъци на системите с асиметрично криптиране:

- Значително по-бавни в сравнение със симетричните;
- При използване за криптиране ключът е много по-дълъг от този при симетричните;

Алгоритми на системите с асиметрично криптиране

RSA (Rivest, Shamir, Aldeman - имената на създателите му)

Алгоритъмът се базира на трудността да се разложи едно естествено число на n прости множители. Алгоритъмът е намерил широко приложение в много системи и стандарти (SSL, S-HHT*P*, S-MIME, S/WAN, STT и *P*CT).

В реализирани системи, базирани на този алгоритъм, се ползват ключове с дължина 512, 768, 1024, 2048 бита, но е препоръчително използването минимум на 1024-битови ключа, за да се постигне дълъг срок на надеждност - от няколко месеца до години.

DSA

Алгоритъмът се използва в механизми за създаване на електронен подпис. Представлява вариант на ElGamal криптосхема. Сигурността се основава на трудността на намиране на дискретен логаритъм Zp. Недостатък на тази криптосистема е, че шифрирания текст е два пъти по-дълъг от оригиналния.

ECC (Eliptic Curve Cryptography)

Частен случай на ElGamal криптосхема. Базира се на система, основана на елиптични криви - ECC. Тази криптосистема е описана в стандарта IEEE P1363.

ECC е изключително подходяща криптосистема в ресурсно ограничени изчислителни среди - мобилни устройства, смарт карти и др. ECC в комбинация със симетричните алгоритми 3DES, IDEA и AES се използва за създаване на системи за защита на информация от особено висок клас.

Цифров подпис

- Асиметричното криптиране може да се използва и за автентикация при електронни комунукация или установяване на автентичност на е-документи и верификация за интегритет.
- Днес се използва активно при разпространение на софтуер, финансови трансакции, системи за управление на договори, в данъчната система и др.
- Криптографията, базирана на публични ключове, осигурява надежден метод за цифрово подписване, при който се използват двойки публични и лични ключове.
- Едно лице полага цифров подпис под дадено електронно съобщение (файл, документ, e-mail и др.) чрез личния си ключ. Разгледано технически цифровото подписване на едно съобщение се извършва на две стъпки. На първата стъпка се изчислява хеш стойност на съобщението (message digest) по някакъв криптографски алгоритъм за хеширане (например MD4, MD5, SHA1 или друг).
- На втората стъпка от цифровото подписване получената в първата стъпка хеш стойност на съобщението се шифрира с личния ключ, с който се извършва подписването. За целта се използва някакъв математически алгоритъм за цифров подпис (digital signature algorithm), който преобразува хеш стойността в шифрирана хеш стойност, наричана още цифров подпис(числов стринг). **Внимание! Цифровото подписване на документ или електронна комуникация не го/я криптира.**

Цифров подпис

- Полученият цифров подпис обикновено се прикрепя към съобщението в специален формат, за да може да бъде верифициран на по-късен етап, когато това е необходимо.
- Цифровият подпис позволява на получателя на дадено подписано съобщение да провери истинския му произход и неговата цялостност (интегритет). Процесът на **проверка (верификация) на цифров подпис** има за цел да установи дали дадено съобщение е било подписано с личния ключ, който съответства на даден публичен ключ.
- Проверката на цифров подпис не може да установи дали едно съобщение е подписано от дадено лице. За да проверим дали едно лице е подписало дадено съобщение, е необходимо да се сдобием с истинския публичен ключ на това лице. Това е възможно или чрез получаване на публичния ключ по сигурен път (например на USB или CD) или с помощта на инфраструктурата на публичния ключ чрез използване на цифрови сертификати.
- Стандарт: Digital Signature Standard (DSS).

Цифров сертификат (Digital certificate)

- Цифровите сертификати се използват за верифициране на самоличността на потребител, независимо подател или получател
- Вид „лична карта“, „шофьорска книжка“
- Представлява файл с информация за потребителя
- Генерира се от CA (Certifying Authority) и включва 4 стъпки:

1. Key Generation,
2. Registration,
3. Verification,
4. Creation.

- В основата стои т.нар. Public Key Infrastructure
- Позволява изграждане на криптирана връзка между клиента и сървъра

PKI (Public Key Infrastructure)

- В криптографията PKI е споразумението, което свързва определен публичен ключ с идентичността на неговия собственик (титуляр) с помощта на сертифициращ орган (Certificate Authority или CA).
- Еднозначността на свързването се гарантира от сертифициращия орган, чрез строго установен процес на регистрация и издаване на цифровия сертификат (политики за предоставяне на удостоверителни услуги), което може да става както от софтуер, така и от човек.
- Органът, който осигурява тази еднозначна свързаност, се нарича регистриращ орган (Registration Authority или RA) и представлява звено на сертифициращия орган, осъществяващо дейностите по приемане, проверка, одобряване или отхвърляне на исканията за издаване на сертификати.
- Друг участник в PKI е проверяващият орган (Vertification Authority или VA). В издадения от сертифициращия орган сертификат с публичен ключ са кодирани редица атрибути, като идентичност на титуляра, самият публичен ключ, тяхната връзка, условията за валидност и др. по начин, който гарантира че не могат да бъдат фалшифицирани.
- Използват се X.509 сертификати. Един X.509 цифров сертификат съдържа публичен ключ на дадено лице, информация за това лице (име, организация и т. н.), информация за сертификационния орган, който е издал сертификата, информация за срока му на валидност, информация за използваните криптографски алгоритми и различни други детайли.

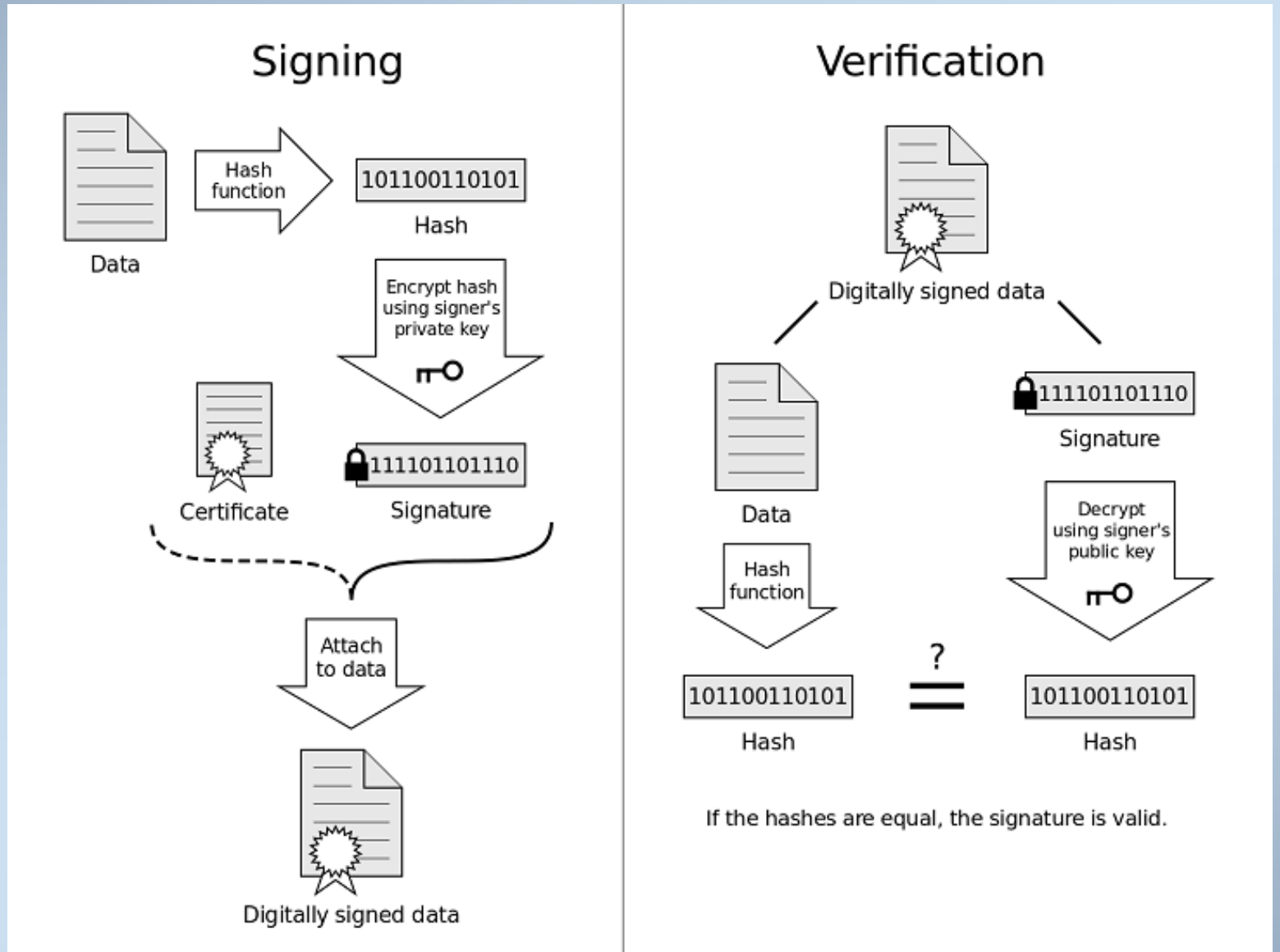
Пример - сертификат

Owner: CN=www.frank4dd.com, EMAILADDRESS=public@frank4dd.com, OU=Support, O=Frank4DD, ST=Tokyo, C=JP
Issuer: EMAILADDRESS=support@frank4dd.com, CN=Frank4DD Web CA, OU=WebCert Support, O=Frank4DD, L=Chuo-ku, ST=Tokyo, C=JP
Serial number: e1e
Valid from: Sat Jan 03 09:00:01 JST 1 until: Sat Jan 01 08:59:59 JST 10000
Certificate fingerprints:
MD5: 00:3F:5B:4C:EC:0D:C0:3D:E5:D8:1F:8D:E1:5E:31:A8
SHA1: DB:17:BE:A4:42:88:20:03:C1:31:34:02:B2:49:47:62:0F:54:D5:E0
SHA256:
35:39:2E:95:3F:83:71:2A:D1:49:EB:EA:65:DD:BA:6A:AD:03:0B:3F:18:6C:E1:46:8C:A5:6C:F8:4C:69:BB:8C
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:
...

Заедно подпис+сертификат

https://cheapsslsecurity.com/blog/digital-signature-vs-digital-certificate-the-difference-explained/



Практически методи за криптиране на данни

- Много от устройствата които използваме днес използват криптирането за защита на потребителските данни по някакъв начин.
- Full disk encryption (FDE) е един от методите, който разчита на хардуер или софтуер, за да защити цялата информация на целия диск или отделен дял. Криптирането става автоматично на фонов режим. Използва се един единствен ключ.
- File-based encryption (FBE) е друг метод при който се криптират отделни файлове или директории и то с различни ключове наречени File Encryption Key. Криптирането е на ниво файлова система, напр. NTFS.
- Обикновено алгоритъмът, който се използва и в двата случая е Advanced Encryption Standard (AES).

Стандарти – NIST специални публикации

- SP 800-133: DRAFT Recommendation for Cryptographic Key Generation
- SP 800-131A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
- DRAFT SP 800-130: A Framework for Designing Cryptographic Key Management Systems
- SP 800-111: Guide to Storage Encryption Technologies for End User Devices
- SP 800-78-3: Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)
- SP 800-67 Rev. 1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
- SP 800-56B: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
- SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
- SP 800-21 [Second Edition]: Guideline for Implementing Cryptography in the Federal Government

ISO 27002

- БДС ISO/IEC 27002
- Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията
- **12.3.1 Policy on the use of cryptographic controls**
- **12.3.2 Key management Control** Key management should be in place to support the organizations use of cryptographic techniques.
- **15.1.6 Compliance with organizational security policies and technical standards**

COBIT

DS5.8 Policies and procedures for cryptographic key management should manage the lifecycle of keys, including their generation, use, protection, and destruction, and the keys should be properly protected.

Криптоанализ

- **Криптоанализ** (от гръцки κρυπτός — скрит и анализ) — наука за методите на получаване на изходното значение на зашифрована информация, без да е на разположение секретна информация (тоест ключ), необходима за това.
- В повечето случаи под това се разбира намирането, откриването на ключа. В нетехнически смисъл, криптоанализът е взлом върху шифъра (кода). Терминът е бил въведен от американския криптограф Уилям Ф. Фридман през 1920.
- Резултатите от криптоанализа на конкретен шифър се наричат **криптографическа атака** върху този шифър. Успешната криптографическа атака, напълно дискредитираща атакуемия шифър, се нарича взлом или откриване.

Методи за криптоанализ

Честотен анализ

Вероятно първият метод, е така наречения честотен анализ. Той използва статистически данни за езика, на криптираното съобщение. За пример ще вземем английския език. Разполагаме със следното съобщение:

yxszssyqraqkydzdggdutysqaxyqryxszdgrqracgqrayxszdrsoquqwwcgqrayxskyden

В съобщението най-често срещаните букви са „y” и „q”, по 9 пъти, но забелязваме, че най-често срещаното съчетание от три букви е „yxs”, което се среща общо 4 пъти. В английският език, това е “the”, значи „y” е “t”, „x” е “h” и „s” е “e”. Така получаваме следното:

THEzEETqraqkTdzdggdutTEqaHTqrTHEzdgrqracgqraTHEzdrEoquqwwcgqraTHEkTden

Методи за криптоанализ (прод.)

Понеже вече имаме първите две най-срещани букви в английския език, а “q” се среща цели 9 пъти. Следователно, вероятно е „a”.

THEzEETAraqkTdzdggdutTEqaHTqrTHEzdgrqracgqraTHEzdrEoquqwwcgqraTHEkTden

Следващата най-често срещана буква в съобщението е “r”, а в английския език е „O” и т.н. По този начин постепенно се разкрива текстът. Разбира се, колкото е по-дълъг текстът, толкова вероятността за грешка е по-малка. Например, в сегашното съобщение, „e” се среща по-рядко от “t”, с предположението че “q” е „a” се оказва грешно, така че в един момент ще трябва да се върнем назад и да опитаме отново. Всъщност, съобщението е:

„Themeetingistomorrowateightinthemorningbringthemoneyiwillbringthestock”

Статистическите данни за даден език са доста. За английският например, има данни за най-често срещано съчетание от две букви – oo и ee, от три - the, за начална, крайна буква и т.н.

Методи за криптоанализ (прод.)

Метод на Бабидж

- Метод на Бабидж, по-известен като Метод на Казиски, е един добър начин, за разбиване на многоазбучни шифри. Състои се в търсенето на еднакви поредици от символи(3 букви или по-дълги), с цел намиране дължината на ключа. Ето няколко стъпки, чрез които методът се прилага:
- Криптоаналитикът намира всички повтарящи се поредици от символи, като записва през какъв интервал са повторенията. На пример: trskgsxvrnmtrsp
- Тук „trs" се повтаря през 10 символа. Проверяваме интервала между повторенията за колкото се може повече групи в текста, така ще можем да сме по-сигурни.
- Внимателно оглеждаме интервалите, ако някой преобладава, то вероятно това е дължината на ключа, а ако не, то е кратно на дължината на ключа. От горния пример, нека по-нататък в съобщението имаме повторение през 15 символа. Така имаме 10 и 15, следователно ключът трябва да е делител на 10 и на 15, значи е 5. При по-дълъг текст, методът е по-точен, понеже повторения могат да станат и случайно.
- След като знаем дължината на ключа, която е l, разглеждаме съобщението като l съобщения, криптирани с прост Цезаров Шифър.
- След като е разкриптирал съобщението, аналитикът може да използва получените открит-текст и ширования-текст за да намери ключа, и да разбива и останалите съобщения от кореспонденцията, ако се криптират със същия ключ.

Заключение

- Криптографията е метод за зашита на информацията.
- В днешни условия това е от изключителна важност поради използването на големи обеми информация дори и от обикновените хора.
- Тенденциите на увеличаване на този обем обуславят и нарастването на средствата и усилията за криптиране на чувствителната информация в ежедневните дейности.
- Така например съвременните мобилни платформи и приложения(напр. за комуникация) изцяло кодират информацията с която работят.

Софтуерна рамка за криптографски услуги

CryptoMañana (CryptoManana) е PHP криптографска рамка, която предоставя обектно-ориентирани решения за повишаване на сигурността на вашия проект. Кодовата база на проекта следва принципите на S.O.L.I.D/KISS/DRY и изпълнява няколко популярни шаблона за проектиране на софтуер. Софтуерната рамка предоставя напълно функционален криптографски модел с огромно количество криптивни примитиви, протоколи и услуги. Той е много полезен за сигурно хеширане, криптиране, обмен на ключове, подписване на данни, генериране на произволни данни и дори повече.

Софтуерна рамка за криптографски услуги

Пароло-базирана автентикация;

Симетрично-базирана автентикация;

Асиметрично-базирана автентикация;

Услуга за размяна на ключове;

Удостоверено шифроване;

Много-пасово криптиране;

Генериране на цифров подпис;

Протокол за криптографски цифров плик.

Услуга за сигурно псевдо-случайно разбъркване на информация;

Услуга за сигурен псевдо-случаен избор на елементи от информация;

Услуга за сигурно псевдо-случайно генериране на криптографски низове;

Услуга за сигурно изтриване на информация от физически устройства чрез стандарта DOD 5220.22-M.

Софтуерна рамка за криптографски услуги - примитиви

- Квази-генератор - QRNG;
- Псевдо-генератор - PRNG;
- Криптографски псевдо-генератор – CSPRNG;
- Заличаване на данни - DOD 5220.22-M.
- MD5, HMAC-MD5, HKDF-MD5, PBKDF2-MD5;
- SHA-1, HMAC-SHA-1, HKDF-SHA-1, PBKDF2-SHA-1;
- SHA-2-224, HMAC-SHA-2-224, HKDF-SHA-2-224, PBKDF2-SHA-2-224;
- SHA-2-256, HMAC-SHA-2-256, HKDF-SHA-2-256, PBKDF2-SHA-2-256;
- SHA-2-384, HMAC-SHA-2-384, HKDF-SHA-2-384, PBKDF2-SHA-2-384;
- SHA-2-512, HMAC-SHA-2-512, HKDF-SHA-2-512, PBKDF2-SHA-2-512;
- SHA-3-224, HMAC-SHA-3-224, HKDF-SHA-3-224, PBKDF2-SHA-3-224;
- SHA-3-256, HMAC-SHA-3-256, HKDF-SHA-3-256, PBKDF2-SHA-3-256;
- SHA-3-384, HMAC-SHA-3-384, HKDF-SHA-3-384, PBKDF2-SHA-3-384;
- SHA-3-512, HMAC-SHA-3-512, HKDF-SHA-3-512, PBKDF2-SHA-3-512;
- RIPEMD-128, HMAC-RIPEMD-128, HKDF-RIPEMD-128, PBKDF2-RIPEMD-128;
- RIPEMD-160, HMAC-RIPEMD-160, HKDF-RIPEMD-160, PBKDF2-RIPEMD-160;
- RIPEMD-256, HMAC-RIPEMD-256, HKDF-RIPEMD-256, PBKDF2-RIPEMD-256;
- RIPEMD-320, HMAC-RIPEMD-320, HKDF-RIPEMD-320, PBKDF2-RIPEMD-320;
- WHIRLPOOL, HMAC-WHIRLPOOL, HKDF-WHIRLPOOL, PBKDF2-WHIRLPOOL;

Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата понятия, дефиниции и аспекти. Търсенето може да направите и на чужди езици, които владеете.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Посочете Вашият опит с криптографията.
- Проучете за всяко от устройствата които използвате кой практически метод за криптиране се използва за целия диск или за отделни файлове или папки.