International Science Group

THEORETICAL AND SCIENTIFIC FOUNDATIONS OF ENGINEERING

MONOGRAPH

DOI 10.46299/ISG.2020.MONO.TECH.II
ISBN 978-1-64945-873-5
BOSTON (USA) – 2020

ISBN - 978-1-64945-873-5
DOI- 10.46299/isg.2020.MONO.TECH.II

Theoretical and scientific foundations of engineering

Collective monograph

Boston 2020

Library of Congress Cataloging-in-Publication Data

ISBN - 978-1-64945-873-5
DOI - 10.46299/isg.2020.MONO.TECH.II

Authors - Apostolova R., Shembel E., Aurbach D., Markovsky B., Kovalskyi Bohdan, Holubnyk Tetyana, Zanko Nataliya, Pysanchyn Nadiia, Azarova Anzhelika, Azarova Larysa, Rosol Nataliia, Bystritskiy Oleksander, Kovalenko Igor, Antipova Kateryna, Davydenko Yevhen, Shved Alyona, Bronnikova Sofya, Yakovenko Ihor, Bakulin Yevhenii, Bakulina Valentyna, Zhuk Volodymyr, Matlai Ivan, Popadiuk Ihor, Vovk Lesya, Zhuk Volodymyr, Mysak Ihor, Kochmarskii Volodymyr, Gayevskii Valerij, Riabenko Oleksandr, Borsukovskyi Yurii, Tkachenko Valentyna, Lebid Iryna, Luzhanska Nataliia, Zamorska Iryna, Volkova Tatyana, Abramova Liudmyla

Published by Primedia eLaunch
https://primediaelaunch.com/

Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe and Ukraine. The articles contain the study, reflecting the processes and changes in the structure of modern science.

The recommended citation for this publication is:
Theoretical and scientific foundations of engineering: collective monograph / Apostolova R., Shembel E., Aurbach D., Markovsky B., – etc. – International Science Group. – Boston : Primedia eLaunch, 2020. 180 p. Available at : DOI : 10.46299/isg.2020.MONO.TECH.II

TABLE OF CONTENTS

SECTION 2 COMPUTER AND SOFTWARE ENGINEERING

2.1 models and methods of electronic digital signature

Технологія застосування систем ЕЦП є сьогодні найбільш прийнятним способом візування документації, особливо за необхідності ведення документо-обігу в умовах коронавірусної пандемії. Таким спосіб розрахований на мережу абонентів, що посилають один одному електронні документи, наприклад платіжні доручення [19]. Абонентами можуть бути клієнти банку і сам банк у системі клієнт– банк або банки під час обміну документами в міжбанківської мережі. Деякі з цих абонентів можуть тільки перевіряти підписані іншими повідомлення, інші (назвемо їх абонентами з правом підпису) можуть як перевіряти, так і підписувати повідомлення. Крім того, можуть бути випадки, коли хто-небудь може ставити свій ЕЦП тільки як другий підписант після підпису певного абонента-начальника (наприклад, директор бухгалтер); це не змінює суті справи.

Розглянемо далі, такі можливі дві ситуації: перша – якщо в цій мережі є центр (абонент, наділений особливими повноваженнями), друга – всі абоненти з правом підпису рівноправні. Не виключеною є і ситуація, за якої функції центру виконують кілька «локальних центрів». У мережах із центрами можуть бути закладені різні ступені «довіри» центру до абонентів. Тобто, центри в мережах можуть (потенційно) або повністю контролювати абонента, або виконувати чисто формальні функції адміністрування.

Перед підписуванням необхідно передбачити певні запобіжні заходи. У разі програмної реалізації, як правило, секретний ключ підписанта зберігається на його особистій флеш-картці, захищеної від копіювання. Однак цього буває недостатньо, адже флеш-карту можуть викрасти або просто втратити. Отже, необхідний захист від несанкціонованого доступу до секретної інформації

(ключа). Природним вирішенням цієї проблеми є парольний захист. Паролем можуть захищатися не лише функції (опції) поставлення підпису і генерації ключів, а й функції, що змінюють вміст каталогу відкритих ключів абонентів мережі й ін.

У разі програмної реалізації необхідно перевірити відсутність у системі «криптовірусов», які можуть завдати істотної шкоди. Наприклад, в момент підписання «крипто віруси» можуть перехопити секретні ключі і скопіювати їх. Крім того, під час перевірки підпису вони можуть змусити систему «повідомити», що підпис є вірним, хоча він, насправді, є неправильним. Можливим є криптовірус, який, потрапивши в систему одноразово під час генерації ключів, змусить систему згенерувати слабкі ключі. Наприклад, якщо ключі генеруються на основі датчика випадкових чисел, який використовує вбудований таймер, вірус може змінити свідчення таймера, а потім відновити «статус кво». Згодом ці ключі можуть бути легко розкриті зловмисником. Проти таких криптовірусів є лише один захист – завантаження з «чистого» системного носія інформації, і використання «чистого» програмного продукту.

Для створення ЕЦП для конкретного документу необхідно виконати такі два етапи.

1. Генерація ключів. На цьому етапі для кожного абонента генерується пара ключів: секретний і відкритий. Секретний ключ зберігається абонентом у таємниці. Він використовується для формування підпису. Відкритий ключ пов'язаний із секретним особливим математичним співвідношенням і є відомим усім іншим користувачам мережі та призначений для перевірки підпису. Його слід розглядати як необхідний інструмент для перевірки, що дозволяє визначити автора підпису і достовірність електронного документа, але не дозволяє обчислити секретний ключ.

Можливі два варіанти проведення цього етапу. Природним є варіант, коли генерацію ключів абонент може здійснювати самостійно. Не виключено, однак, що в певних ситуаціях цю функцію доцільно передати центру, який буде виробляти для кожного абонента пару ключів секретний і відкритий і займатися

їх поширенням. Другий варіант має ряд переваг адміністративного характеру, однак має принципову ваду – у абонента немає гарантії, що його особистий секретний ключ є унікальним і центр може підробити будь-який підпис.

2. Підписання документа. Перш за все, документ «стискають» до кількох десятків або сотень байтів за допомогою так званої хеш-функції, значення якої складним чином залежить від змісту документа, але не дозволяє відновити сам документ. До отриманого значення хеш-функції застосовують певне математичне перетворення (залежно від обраного алгоритму ЕЦП) і отримують підпис документа. Цей підпис може бути складеним із читаних символів (букв), але часто його представляють у вигляді послідовності довільних символів, що «не читаються». ЕЦП може зберігатися разом із документом, наприклад, стояти на початку або в кінці, або в окремому файлі.

Під час перевірки підпису перевіряючий повинен послугуватися відкритим ключем абонента, який поставив підпис. Цей ключ повинен бути аутентифіко-ваним, тобто перевіряючий повинен бути повністю впевнений, що даний ключ відповідає саме тому абоненту, який видає себе за його власника. Якщо абоненти самостійно обмінюються ключами, ця впевненість може підкріплюватися зв'язком по телефону, особистим контактом або в інший спосіб. Якщо ж абоненти діють в мережі з виділеним центром, їх відкриті ключі підписуються (сертифікуються) центром і безпосередній контакт абонентів між собою (під час перевання або підтвердження автентичності ключів) замінюється контактами кожного з них окремо з центром [20].

Процедура перевірки підпису складається з двох етапів: обчислення хеш-функції документа і проведення математичних обчислень, які визначаються алгоритмом підпису. Останні полягають у перевірці того чи іншого співвідношення, що зв'язує хеш-функцію документа, підпис під цим документом і відкритий ключ підписала абонента.

Якщо розглянуте співвідношення виявляється виконаним, то підпис визнається правильним, а сам документ справжнім, у протилежному випадку документ вважається зміненим, а підпис – недійсним.

Система ЕЦП повинна вирішувати завдання запобігання підробки підпису. У США був прийнятий стандарт на електронний підпис, який є необхідним, по-перше, для отримання впевненості в тому, що зроблений відповідно до стандарту засіб реалізації ЕЦП є крипостійким, по-друге, стандарт забезпечує патентну чистоту, зокрема, алгоритм RSA запатентований в США.

Стійкість більшості схем ЕЦП залежить від стійкості асиметричних алгоритмів шифрування та хеш-функцій. Існує така класифікація атак на схеми ЕЦП:

– атака з відомим відкритим ключем;

– атака відомими підписаними повідомленнями – супротивник, крім відкритого ключа має і набір підписаних повідомлень;

– проста атака з вибором підписаних повідомлень – супротивник має можливість вибирати повідомлення, при цьому відкритий ключ він отримує після вибору повідомлення;

– спрямована атака з вибором повідомлення;

– адаптивна атака з вибором повідомлення.

Кожна атака переслідує певну мету, які можна розділити на кілька класів:

– повне розкриття – супротивник знаходить секретний ключ користувача;

– універсальна підробка – супротивник знаходить алгоритм, функціонально аналогічний алгоритму генерації ЕЦП;

– селективна підробка – підробка підпису обраного повідомлення;

– екзистенційна підробка – підробка підпису хоча б для одного випадково обраного повідомлення;

На практиці застосування ЕЦП дозволяє виявити або запобігти таким діям порушника:

– відмова одного з учасників від авторства документа;

– модифікація прийнятого електронного документа;

– підробка документа;

– нав'язування повідомлень у процесі передавання – супротивник

перехоплює обмін повідомленнями і модифікує їх;

– імітація передавання повідомлення.

Так само існують порушення, від яких неможливо захистити систему обміну повідомленнями – це повтор передавання повідомлення і фальсифікація часу відправлення повідомлення. Протидія даним порушенням може ґрунтуватися на використанні тимчасових вставок і суворому обліку вхідних повідомлень.

Будь-який метод автентифікації, який базується на технології відкритого ключа, може бути перетворений у метод цифрового підписування шляхом заміни перевіряльника однонаправленою хеш-функцією. При цьому повідомлення не хешується перед підписанням, а замість цього хеш-функція включається у саму схему цифрового підписування. Таким чином, у схеми цифрового підписування можуть бути перетворені відомі схеми автентифікації сторін взаємодії, зокрема RSA, Ель-Гамаля, Фіата-Шаміра, Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра.

Варіант реалізації електронного цифрового підпису, побудованого на алгоритмі RSA, наведено на рис. 1.

На відміну від алгоритму шифрування відправником тут є власник пари закритий / відкритий ключ. Процедура формування електронного підпису *sign* під повідомленням схожа з шифруванням документа, але в міру закритого ключа *d* за відліком *n* зводиться не саме повідомлення або його частини, а дайджест повідомлення *h*. Невід'ємною частиною алгоритмів ЕЦП є хешування інформації, на рис. 1 він позначений через *H*.

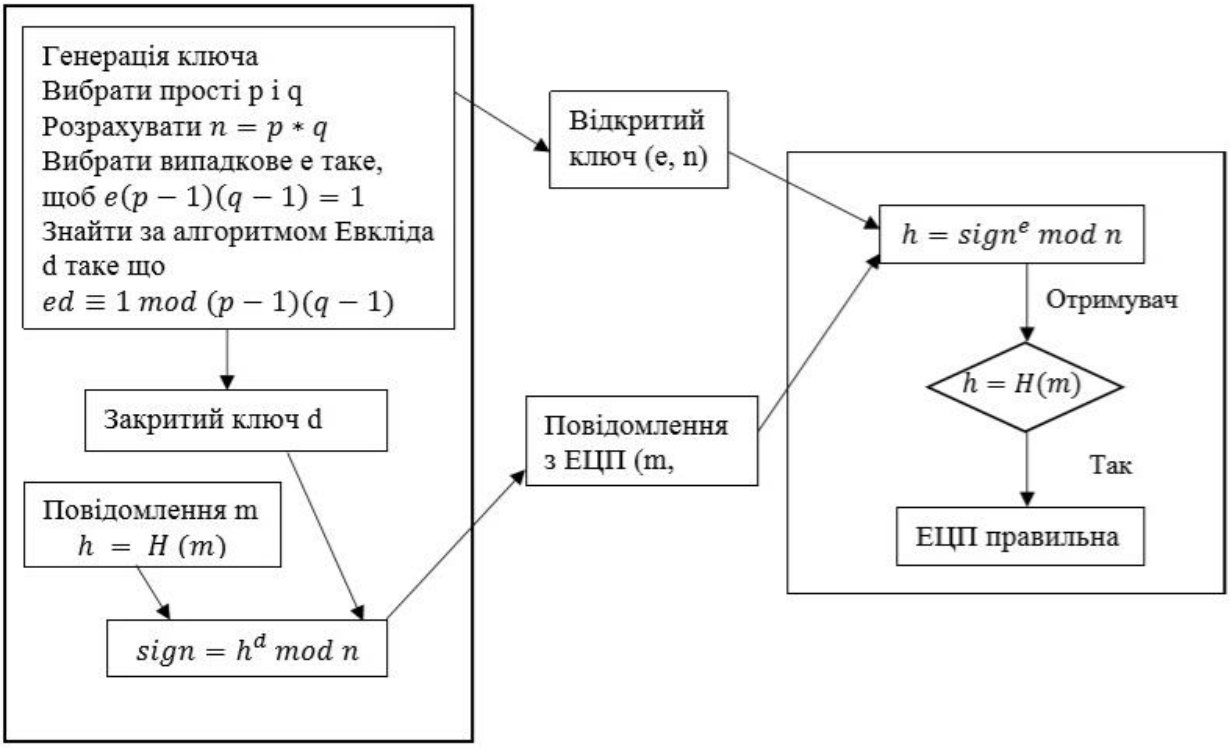


Рисунок 1. Реалізація електронного цифрового підпису, що побудований на алгоритмі RSA

Повідомлення *m* з підписом *sign* буде однозначно аутентифікованим. Авторство повідомлення може бути встановлено і доведено парою ключів (*d*, *e*) з використанням сертифікації. Зловмисник не зможе підмінити повідомлення *m* (точніше, йому буде дуже важко це зробити), оскільки йому необхідно замість повідомлення *m* підставити інше повідомлення *m'*, яке задовольняє його і має таке ж значення хеш-функції, що і у *m*, що є на сьогодні обчислювально складним завданням. Із цієї ж причини зловмисник не зможе застосувати перехоплений підпис *sign* для підпису іншого документа, оскільки для іншого документа буде отримано інше значення хеш-функції *h*, а воно знаходиться в основі підпису. Таким чином, всі необхідні властивості підпису описаним алгоритмом забезпечуються, що ж стосується криптостійкісті методу ЕЦП, то вона визначається криптостійкістю використовуваного асиметричного криптографічного методу і функції односпрямованого шифрування. Необхідно відзначити також, що саме повідомлення *m* передається у відкритому вигляді.

Для того, щоб забезпечити конфіденційність інформації, що передається, потрібне використання додаткового шифрування за симетричною або асиметричною схемою (при цьому шифрування на ключі *d* конфіденційності не забезпечить, оскільки повідомлення може бути розшифровано відкритим ключем).

Дуже популярними є схеми ЕЦП на основі алгоритму Ель-Гамаля, що зумовлюється як належною стійкістю алгоритму, так і кращою, порівняно з RSA, швидкістю обчислень. Зокрема, в стандарті національного інституту стандартів США DSS (Digital Signature Standard) використовується алгоритм DSA (Digital Signature Algorithm), який є варіацією алгоритму ЕЦП Ель-Гамаля в модифікації Шнорра. В алгоритмі використовуються такі відкриті параметри:

p – просте число в діапазоні від 512 до 1024 біт;

q – 160-бітове просте число, дільник $p-1$;

v – будь-яке число, $v < p-1$, таке, що $v(p-1)/q \bmod p > 1$;

$g = v(p-1)/q \bmod p$;

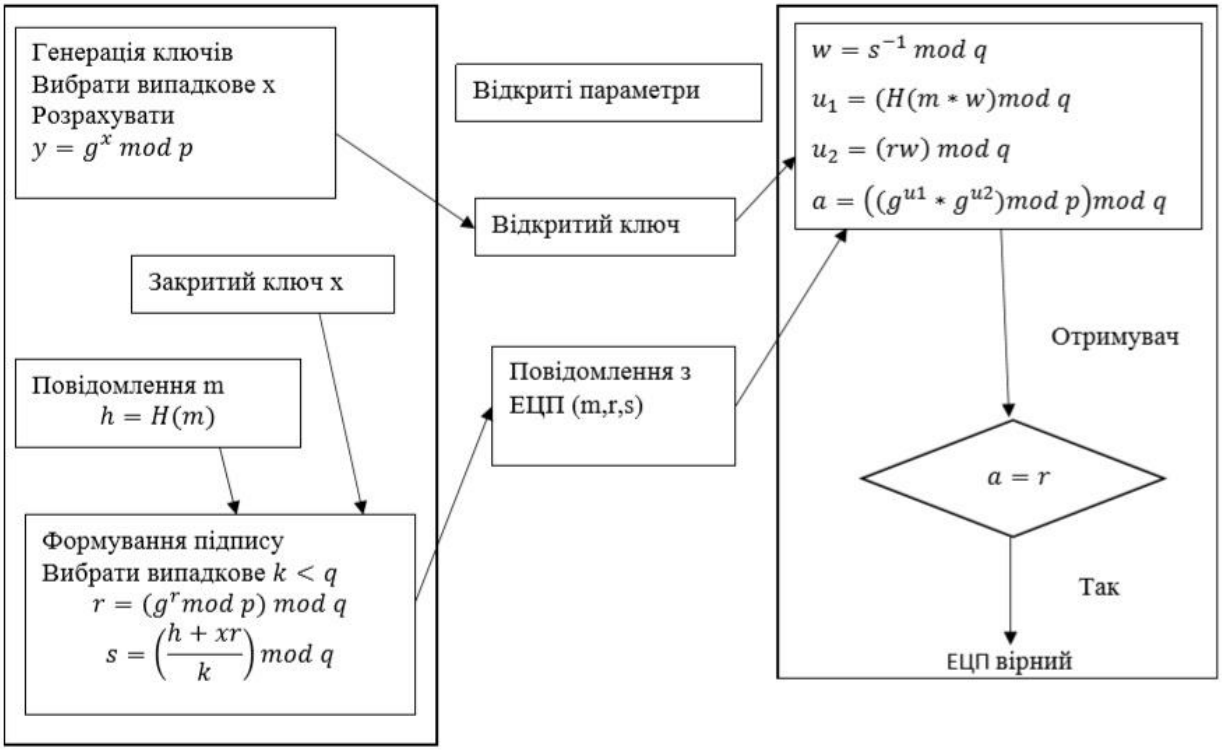
$y = g^x \bmod p$.

Секретним ключем є будь-яке 160-розрядне число *x*, $x < q$.

Алгоритм ЕЦП DSA у графічній формі представлено на рис. 2.

Існує безліч модифікацій схеми Ель-Гамаля: це алгоритми DSA, ECDSA, KCDSA, схема Шнорр. Так, наприклад, алгоритм RSA, заснований на складному процесі факторизації великих чисел, є одним із перших асиметричних алгоритмів, а алгоритм DSA заснований на складному дискретному логарифмуванні в кінцевому полі, прийнятий за державний стандарт США, застосовується для секретних і несекретних комунікацій. Одним із типів модифікації стало перенесення обчислень в групу, утворену еліптичними кривими.

Для практичного застосування в криптографії використовуються еліптичні



Ри

сунок 2. Алгоритм ЕЦП DSA в графічній формі

криві (ЕК), задані над полями Галуа.

Нехай задано просте число p>3. Тоді *e* еліптичної кривої *E*, визначеної над простим кінцевим полем *Fp*, називається безліч пар чисел (*x*, *y*), *x*, *y* ∈ *Fp*, які задовольняють тотожності:

$$y^2 = x^3 + ax + b \bmod p$$

де $a, b \in Fp$ і $(4a^3 + 27b^2) \neq 0 \bmod p.$

Крім того, до еліптичної кривої додається нескінченно віддалена точка I. Таким чином, точки, що задовольняють рівняння кривої *E*, і точка *I* утворюють кінцеву абелеву групу. Геометричне уявлення еліптичної кривої зображено на рис. 3.

Для точок еліптичної кривої визначена операція додавання. Для двох точок, що належать кривій *E*, *P* (*xp*, *yp*) і *Q* (*xp*, *yp*), точка, яка є їхньою сумою, також буде лежати на еліптичній кривій. Координати точки $S = P + Q$ визначаються такими виразами:

$$k = yq - \frac{yp}{xq - xp} \bmod p,$$

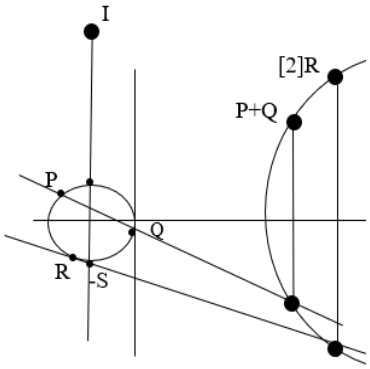


Рисунок 3 – Графік еліптичної кривої *ЕК*, заданої над полями Галуа

$$xs = k^2 - xq - xp \bmod p,$$

$$ys = k * (xq - xp) - yp \bmod p.$$

Точку *S* можна отримати графічно шляхом нескладних побудов. Для цього на графіку проводиться пряма через точки *P* і *Q*, і точка перетину цієї прямої з *ЕК* дзеркально відображається щодо осі *OX* (див. рис 3). Якщо точки P і Q збігаються, то ми отримуємо точку $S = 2 * Q$. Тоді її координати визначаються інакше:

$$k = 3 * xq^2 + \frac{a}{2*yp} \bmod p\ ,$$

$$xs = k^2 - 2xq \bmod p,$$

$$ys = k(xq - xp) - yp \bmod p\ .$$

Графічно подвоєння точки можна отримати, побудувавши дотичну до точки і відбивши точку перетину дотичної з еліптичної кривої щодо осі *OX* (див. точки *R* і [21]R на рис. 3). Звідси очевидно, що можна визначити операцію множення деякої точки еліптичної кривої на ціле число, яка дозволяє визначити точку *Q = k * P* (точка *P*, помножена на ціле число *k*, звертається в точку *Q*). Скалярне множення здійснюється за допомогою кількох комбінацій складання і подвоєння точок еліптичної кривої. Наприклад, точка 25 * *P* може бути представлена, як

$$25 * P = 2 * (2 * (2 * (2 * P)) + 2 * (2 * (2 * P))) + P\ .$$

З операцією множення точки *ЕК* на ціле число безпосередньо пов'язана надійність і криптостійкість еліптичної криптографії. Справа в тому, що завдання ECDLP (Elliptic Curve Discrete Logarithm Problem – задача

дискретного логарифма на еліптичній кривій), суть якого полягає в пошуку цілого числа k за відомими точкам P і $Q = k * P$, є важким. Крім рівняння, важливим параметром кривої є базисна (генеруюча) точка G, що обирається для кожної кривої окремо. Секретним ключем відповідно до технології ЕК є велике випадкове число k, а відкритим ключем – добуток k і базисної точки G.

На криптостійкість алгоритму істотно впливає правильний вибір як самої кривої (коефіцієнтів a, b, p), так і базисної точки G [22].

Не кожна крива забезпечує необхідну криптостійкість і для деяких із них завдання ECDLP вирішується досить ефективно. Оскільки невдалий вибір кривої може спричинити за собою зниження забезпечується рівня безпеки, організації по стандартизації виділяють цілі блоки кривих, що володіють необхідною надійністю. Використання стандартизованих кривих рекомендується і тому, що стає можливою найкраща сумісність між різними реалізаціями протоколів інформаційної безпеки.

SECTION 3 COMPUTER SCIENCE

3.1 assessment of the information load on managers in complex linear-functional organizational structures

Modern high-tech enterprises implement organizational management structures that are characterized by strict hierarchy and uneven distribution of all kinds of information (concerning technology, management, communication etc.) between departments. Analysis of the information load on the elements of the structure, especially the upper levels of the hierarchy (senior managers), can be performed using models for evaluation of information flows in the structure and its subsequent optimization.

A number of publications have been devoted to the development of models and methods for analysis of information flows, resources and processes. The work [23] describes the principles of building a control system and of management of organizational processes that take into account the accumulated information. The work [24] is devoted to the development of an information flows model in an automated control system using the theory of random processes. The method of intellectual management of information resources of an industrial enterprise is described in [25,26]. Based on the performed analysis, the authors consider the amount of publications devoted to the issues of modeling information flows in organizational structures to be insufficient.

The model of a complex linear-functional organizational structure (CLFOS) can be presented as a sequence of hierarchically ordered levels of control (see figure 1). A complex organizational structure is required to have more than 1000 workers and at least 3 hierarchy levels.