



УКРАЇНА

(19) **UA** (11) **96173** (13) **U**
(51) МПК (2015.01)
G07D 7/00
H04L 9/30 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2014 05061**
(22) Дата подання заявки: **13.05.2014**
(24) Дата, з якої є чинними права на корисну модель: **26.01.2015**
(46) Публікація відомостей про видачу патенту: **26.01.2015, Бюл.№ 2**

(72) Винахідник(и):
Комаров Володимир Олександрович (UA),
Сайко Володимир Григорович (UA),
Бугера Михайло Григорович (UA),
Овсяннікова Тетяна Миколаївна (UA),
Сендецький Микола Миколайович (UA),
Куровська Тетяна Юріївна (UA),
Сальнікова Ольга Федорівна (UA),
Качмар Дмитро Михайлович (UA),
Владімірова Ольга Олегівна (UA),
Кривошей Олександр Валерійович (UA),
Мегенко Андрій Васильович (UA),
Куценко Юрій Олександрович (UA),
Басай Ігор Анатолійович (UA),
Рудич Олексій Володимирович (UA),
Кириленко Денис Олександрович (UA),
Волощенко Євген Сергійович (UA),
Сацик Віталій Сергійович (UA),
Яровий Дмитро Миколайович (UA),
Козленко Микола Володимирович (UA),
Баран Юрій Васильович (UA),
Свердлова Анастасія Дмитрівна (UA),
Шашкін Микита Андрійович (UA),
Волох Олексій Валерійович (UA)
(73) Власник(и):
Комаров Володимир Олександрович,
пров. Щорса, 5-а, кв. 240, м. Київ-133, 01133 (UA),
Сайко Володимир Григорович,
вул. Бальзака, 4, кв. 283, м. Київ-218, 02218 (UA)

(54) СПОСІБ ПЕРЕВІРКИ ДІЙНОСТІ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПISУ, ЩО ЗАВІРЯЄ ЕЛЕКТРОННИЙ ЦИФРОВИЙ ДОКУМЕНТ

(57) Реферат:

Спосіб перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ полягає в тому, що приймають електронний документ, представлений багаторозрядним двійковим числом N , відкритий ключ у вигляді першого g -розрядного і другого f -розрядного двійкових чисел n і α й електронний цифровий підпис у вигляді багаторозрядного двійкового числа S , формують перевірне багаторозрядне двійкове число V , параметри якого порівнюють із параметрами еталонного багаторозрядного двійкового числа, і при їхньому збігу роблять висновок про дійсність електронного цифрового підпису. Для формування перевірного багаторозрядного двійкового числа V електронний цифровий підпис підносять до степеня N по модулю, рівному першому g -розрядному двійковому числу n відкритого ключа, при цьому як

UA 96173 U

еталонне багаторозрядне двійкове число використовують друге f -розрядне число α відкритого ключа.

Корисна модель належить до галузі електрозв'язку й обчислювальної техніки, а саме до галузі криптографічних способів аутентифікації електронних повідомлень, переданих по телекомунікаційних мережах і мережах EOM, і може бути використана в системах передачі електронних повідомлень (документів), завірених електронним цифровим підписом.

Відомий спосіб перевірки електронного цифрового підпису, при якому приймають електронний документ, представлений у вигляді багаторозрядного двійкового числа H , відкритий ключ у вигляді багаторозрядного двійкового числа Y , електронний цифровий підпис у вигляді двох багаторозрядних двійкових чисел s і r , прості багаторозрядні двійкові числа p і q і двійкове число α , що належить до показника q по модулю p , при цьому як багаторозрядне двійкове число приймають електромагнітний сигнал у двійковій цифровій формі, у якому загальне число битів і порядок їхнього проходження відбиває деяке значення двійкового числа, обчислюють два контрольних параметри з використанням вихідних багаторозрядних двійкових чисел p , α , Y , H і S шляхом зведення багаторозрядних двійкових чисел α , Y , r у дискретну степінь по модулю p , порівнюють обчислені контрольні параметри й при їхньому збігу роблять висновок про дійсність електронного цифрового підпису [1].

Недоліком відомого способу є те, що для його проведення потрібен великий часовий інтервал, необхідний для перевірки дійсності електронного цифрового підпису. Це пояснюється необхідністю багаторазового зведення в більший дискретний ступінь по модулю p багаторозрядних двійкових чисел.

Відомий спосіб перевірки електронного цифрового підпису, при якому приймають електронний документ, представлений у вигляді багаторозрядного двійкового числа H , відкритий ключ у вигляді багаторозрядного двійкового числа Y , електронний цифровий підпис у вигляді двох багаторозрядних двійкових чисел s і r , просте багаторозрядне двійкове число p і двійкове число α , що є первісним коренем по модулю p , обчислюють два контрольні параметри з використанням вихідних багаторозрядних двійкових чисел p , α , Y , H і S шляхом зведення багаторозрядних двійкових чисел α , Y , r у дискретну степінь по модулю p , порівнюють обчислені контрольні параметри й при їхньому збігу роблять висновок про дійсність електронного цифрового підпису [2].

Недоліком відомого способу є те, що для його проведення потрібен великий часовий інтервал, необхідний для перевірки дійсності електронного цифрового підпису. Це пояснюється необхідністю багаторазового зведення в більшу дискретну степінь по модулю p багаторозрядних двійкових чисел.

Найбільш близьким технічним рішенням як за суттю, так і за задачею, що вирішується, яке вибрано за найближчий аналог (прототип), є спосіб перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, який полягає в тому, що приймають електронний документ, представлений багаторозрядним двійковим числом H , відкритий ключ у вигляді першого g -розрядного і другого f -розрядного двійкових чисел n і α й електронний цифровий підпис у вигляді багаторозрядного двійкового числа S , формують перевірне багаторозрядне двійкове число B , параметри якого порівнюють із параметрами еталонного багаторозрядного двійкового числа, і при їхньому збігу роблять висновок про дійсність електронного цифрового підпису [3].

Недоліком способу перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, є відносно висока ймовірність несанкціонованого формування електронного цифрового підпису до електронного документа, представленого багаторозрядним двійковим числом H , що має меншу розрядність, ніж у першого g -розрядного двійкового числа n . Це обумовлено тим, що для довільного значення S легко обчислюється значення H , тобто $H = S \cdot \alpha \cdot \text{mod} \cdot n$, що проходить процедуру перевірки дійсності електронного цифрового підпису, тобто буде мати місце "помилкове" підтвердження дійсності електронного цифрового підпису, який завіряє електронний документ.

В основу корисної моделі поставлена задача шляхом зміни процедури формування перевірного багаторозрядного двійкового числа забезпечити зниження ймовірності несанкціонованого формування електронного цифрового підпису - "помилкового" підтвердження дійсності електронного цифрового підпису.

Суть корисної моделі в способі перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, що вибрано за найближчий аналог (прототип), який полягає в тому, що приймають електронний документ, представлений багаторозрядним двійковим числом H , відкритий ключ у вигляді першого g -розрядного і другого f -розрядного двійкових чисел n і α й електронний цифровий підпис у вигляді багаторозрядного двійкового числа S , формують перевірне багаторозрядне двійкове число B , параметри якого порівнюють із параметрами еталонного багаторозрядного двійкового числа, і при їхньому збігу роблять

висновок про дійсність електронного цифрового підпису, полягає в тому, що для формування перевірного багаторозрядного двійкового числа V електронний цифровий підпис підносять до степеня N по модулю, рівному першому g -розрядному двійковому числу n відкритого ключа. Суть корисної моделі полягає і в тому, що як еталонне багаторозрядне двійкове число використовують друге f -розрядне число α відкритого ключа. Суть корисної моделі полягає також і в тому, що інформацію, яка стосується аутентифікації електронних повідомлень, передають по телекомунікаційних мережах і по мережах ЕОМ, включаючи Internet.

Рішення технічної задачі в способі перевірки дійсності електронного цифрового підпису, що завіряє електронний документ (який заявляється), дійсно можливе та досягається тим, що для формування перевірного багаторозрядного двійкового числа V електронному цифровому підписі підносять до степеня N по модулю, рівному першому g -розрядному двійковому числу n відкритого ключа, а також використовують як еталонне багаторозрядне двійкове числа другого f -розрядного двійкового числа α відкритого ключа. Завдяки новій сукупності істотних ознак за рахунок зміни процедури формування перевірного числа досягається зниження ймовірності несанкціонованого формування електронного цифрового підпису, тобто "помилкового" підтвердження дійсності електронного цифрового підпису. Рішення технічної задачі досягається й тим, що інформацію, що стосується аутентифікації електронних повідомлень, передають по телекомунікаційних мережах і по мережах ЕОМ, включаючи Internet, що, у свою чергу, забезпечує правильність і надійність передачі інформації, а так само істотно знижується час передачі повідомлень.

Можливість реалізації заявленого способу пояснюється таким чином. Відомо, що можливість несанкціонованого формування електронного цифрового підпису запобігає тим, що для формування правильного значення електронного цифрового підпису потрібне знання секретного ключа, яким володіє тільки особа, що підписує електронний документ. Відкритий ключ формують залежно від вибраного секретного ключа, завдяки чому забезпечується можливість перевірки дійсності електронного цифрового підпису при використанні тільки відкритого ключа. Однак деякі способи перевірки дійсності електронного цифрового підпису (у тому числі в найближчому аналогу) зберігають відносно високу ймовірність несанкціонованого формування електронного цифрового підпису по відомому відкритому ключу й без використання секретного ключа. Наприклад, у прототипі ця можливість виникає через те, що для довільного багаторозрядного двійкового числа S можна обчислити таке значення N , для якого виконується умова $S \cdot \alpha \bmod n = N$, тобто виявляється можливим сформувати пари значень S і N , при яких забезпечується "помилкове" підтвердження дійсності електронного цифрового підпису.

У технічному рішенні, що заявляється, значною мірою така ймовірність знижується.

Спосіб перевірки дійсності електронного цифрового підпису визначає інші процедури загальної системи електронного цифрового підпису, що у цілому включає процедури формування відкритого й закритого ключів, процедуру генерації електронного цифрового підпису і процедуру перевірки її дійсності. Розглянемо приклад реалізації заявленого технічного рішення в рамках загальної системи електронною цифрового підпису, що включає заявлений спосіб перевірки дійсності електронного цифрового підпису.

Приклад реалізації способу, що заявляється.

При необхідності перевірки дійсності електронного цифрового підпису виконують наступну послідовність дій.

1. Приймають відкритий ключ що підписує (n , α), що розсилається, наприклад, що засвідчує центром по телекомунікаційних мережах. Як приклад нижче прийняті двійкові числа α й n , що мають розрядності $g=332$ $f=331$ відповідно, і наступні послідовності нульових і одиничних битів:

$n = 1001000011111001010110011011011011100110010001111110010000101000$
 $1101100100111111111111111011001010111111010000100110111010010111001$
 $0010111001010111101101011000111001110100011010010011111001010111100$
 $11000111000010010111011100000111010101010001111011011011101100101101$
 $1010011000110001100110011111110111011100011001111111111111011101;$
 $\alpha = 11100100011010010111010100110101000101101010010001000000111001010$
 $110101110100101001010011101110011101111001011111011101010000000001$
 $1000111101011000100110110111100001010011000111010001101000111100001$
 $100110010010011011001000111101000100100110100101101111100110010010$
 $000001010101010001010111101111100010010101010101001101111110.$

2. Приймають електронний документ, представлений, наприклад, що впливає 107-розрядним двійковим числом H (за який може бути взята, зокрема, хеш-функція від електронного документа):

$H = 11100110101000000001001001010101000011011111111110011110000010$
 $11111100100001101001010000001110110000000101.$

3. Приймають електронний цифровий підпис у вигляді 331-розрядного двійкового числа S :

$S = 1101001111101010101101111110110000000010110011011100011000000101$
 $01111010001110101010011100011001110001100010011111000101101110001110$
 $00011001110111001110010011000111010000100011010001101111010101011011$
 $11100011110101110101000111010001001011010010011111001111100111111111$
 $0101101111010111101101111001111100111010110101101001111010010.$

4. Формують перевірне багаторозрядне двійкове число B шляхом зведення електронного цифрового підпису у степінь H по модулю n :

$B = S^H \bmod n = 1110010001101001011101010011010100010110101001000100000$
 $01110010101101011101001010010100111011100111011111001011111101110101$
 $0000000001100011110101100010011011011110000101001100011101000110100$
 $01111000011001100100100110110010001111101000100100110100101101111110$
 $011001001000000101010101000101011110111110001001010101101001101111$
 $1110.$

5. Порівнюють (наприклад, поразрядно) параметри перевірного числа B з параметрами двійкового числа α . Порівняння показує, що параметри багаторозрядних двійкових чисел B і α збігаються, що вказує на дійсність електронного цифрового підпису, тобто прийнятий електронний цифровий підпис ставиться до прийнятого електронного документа, представленому багаторозрядним двійковим числом H , і сформована що підписує, котрому відповідає прийнятий відкритий ключ (n, α) .

Практична реалізація способу перевірки дійсності електронного цифрового підпису, що завіряє електронний документ, що заявляється, з досягненням зазначеного технічного результату можна продемонструвати на наступному прикладі.

Процедури перевірки дійсності електронного цифрового підпису, що завіряє електронний документ, завжди передують дія по формуванню секретного й відкритого ключів, формуванню електронного цифрового підпису і завірненню електронного документа. Сукупність процедур формування секретного й відкритого ключів, формування електронного цифрового підпису і перевірки електронного цифрового підпису становлять загальну систему електронного цифрового підпису [4].

Наведеному вище прикладу реалізації заявленого способу перевірки дійсності електронного цифрового підпису, що завіряє електронний документ, повинні передувати дії по формуванню секретного й відкритого ключів, перетворенню вихідного документа в електронний вид і формуванню електронного цифрового підпису.

5 Зокрема, зазначені етапи загальної системи електронного цифрового підпису, можуть бути реалізовані таким чином:

1. Формують секретний ключ, для чого:

1.1. Генерують (наприклад, за допомогою генератора випадкових чисел) перше випадкове просте число p , наприклад, 133-розрядне:

10

```
p=11010011111000001101001110011100001001010011001101010101010111000
101111001000010011101111100001110010000011110011100110011111000101.
```

1.2. Формують друге випадкове просте число q , для чого:

15 1.2.1. Генерують перші й друге додаткові прості випадкові числа q' і W , наприклад, з розрядністю відповідно 109 і 91:

```
q'=10101011001100101000000011100111001011111100111101100110111001
1111111100110011110001001010001101110100010001 и
W=1000001011110111001010111010111001001111011000101100011011001000
100000101110110010110111000.
```

20 1.2.2. Обчислюють друге випадкове багаторозрядне (у прикладі - 199-розрядне) двійкове число q як збільшене на одиницю добуток перших і другого додаткових випадкових чисел $q=q'+1$:

```
q=101011110010100111110000011001011101001001100111100010011001010001
00010100111110101101110010100111011001011010110111011000011101000110
000000011000000101010100110110110011010101000111011001100100111001.
```

25 Сформована трійка випадкових багаторозрядних двійкових чисел p , q і q' становить секретний ключ.

2. Формують відкритий ключ у вигляді першого g -розрядного і другого f -розрядного чисел n і α , для чого:

30 2.1. Обчислюють перше g -розрядне (у нашій прикладі 332-розрядне) двійкове число n як добуток чисел p і q , що входять у секретний ключ:

```
n=1001000011111001010110011011011011100110010001111110010000101000
1101100100111111111111111011001010111111010000100110111010010111001
0010111001010111101101011000111001110100011010010011111001010111100
11000111000010010111011100000111010101010001111011011011101100101101
1010011000110001100110011111110111011100011001111111111111011101.
```

35 2.1. Формують друге f -розрядне (у нашому прикладі 331-розрядне) двійкове число α , для чого:

2.2.1. Генерують випадкове двійкове, наприклад 270-розрядне, число p :

```

β=10110111000000001001110010001101010011000001010100001011110111010
0010111110110011110100100110111011000001100000111001000011111001110
000110100100001101010000000001011100001001001010111011110111100111
1100000111110011010100001100000100100110001101011101010101110000000.

```

2.2.2. Обчислюють функцію Ейлера $\varphi(n)=(p-1)(q-1)$ від першого g -розрядного двійкового числа n :

5

```

φ(n)=100100001111100101011001101101101110011001000111111001000010100
011011001001111111111111101100101011111101000010011011101001011100
01101011011000010110001010010100010100010000000011011010011000011011
01100101101011100010111010011000101110100000000001100111100100100111
1101111000000010011001010010101111111111101011011001011011100000.

```

2.2.3. Обчислюють додатковий параметр t шляхом розподілу функції Ейлера $\varphi(n)$ на перше додаткове просте випадкове число q' , тобто

10

```

t = φ(n)/q' = 1101100011001001011110110001000011111101001101100100110001
00110001000101111011001110011010101111010010100000010100100010110011
10001110001010110001110111000101100001111101000111100101010011101000
10001010010011010100011100000.

```

2.2.4. Обчислюють друге f -розрядне (у нашому прикладі 331-розрядне) двійкове число α шляхом зведення двійкового числа β у степінь t по модулю n , тобто $\alpha=\beta \cdot t \bmod n$:

15

```

α = 11100100011010010111010100110101000101101010010001000000111001010
110101110100101001010011101110011101111001011111011101010000000001
1000111101011000100110110111100001010011000111010001101000111100001
1001100100100110110010001111101000100100110100101101111100110010010
0000010101010100010101111011111000100101010101010011011111110.

```

3. Перетворюють вихідний документ в електронний вид, наприклад, шляхом перекладу буквених символів у багаторозрядне двійкове число, що потім представляють у вигляді 107-розрядної хеш-функції H :

20

```

H = 11100110101000000001001001010101000011011111111110011110000010
1111110010000110100101000000110110000000101.

```

4. Формують ЕЦП, для чого:

25

4.1. Попередньо обчислюють 107-розрядне двійкове число K , що є зворотним до H по модулю q' , тобто $K \cdot H \bmod q'=1$:

```

K = 1101100111111111000110000001110111000001001011000110110010010000
1011000101111001101100110111100011101100010.

```

30

4.2. Обчислюють електронний цифровий підпис (у прикладі - 331-розрядне двійкове число) за формулою $S=\alpha \cdot K \bmod n$:

```

S = 1101001111101010101011111110110000000010110011011100011000000
10101111010001110101010011100011001110001100010011111000101101110001
11000011001110111001110010011000111010000100011010001101111010101011
0111110001111010111010100011101000100101101001001111100111100111111
11101011011110101111011011110011111100111010110101101001111010010.

```

Таким чином, на етапах, що передують процедурі перевірки дійсності електронного цифрового підпису, отримані у вигляді багаторозрядних двійкових чисел (цифрових двійкових електромагнітних сигналів):

- секретний ключ у вигляді трьох двійкових чисел: 133-розрядного p , 199-розрядного q і 109-розрядного q' ;

- відкритий ключ у вигляді двох двійкових чисел: 332-розрядного n і 331-розрядного α ;

- електронний цифровий підпис у вигляді 331-розрядного двійкового числа S ,

- електронний документ, хеш-функція від якого представляє 107-розрядне двійкове число H . Сформований відкритий ключ і електронний цифровий підпис дозволяють однозначно встановити шляхом здійснення процедури перевірки дійсності електронного цифрового підпису за способом, який заявляється, що при формуванні електронного цифрового підпису був використаний секретний ключ, тобто що підпис є справжньою й ставиться до електронного документа, представленою у вигляді багаторозрядного двійкового числа H .

Дійсно, відповідно до способу перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, що заявляється, дійсність електронного цифрового підпису встановлюється при виконанні умови, а саме: $S \cdot H \bmod n = \alpha$.

Для розглянутих у прикладі реалізації способу, що заявляється, багаторозрядних двійкових чисел ця умова виконується, тому що:

$$\begin{aligned}
 S^H \bmod n &= (\alpha^K)^H \bmod n = (\alpha^{H^1})^H \bmod n = \alpha^{H^{-1}H} \bmod n = \\
 &= \alpha^{H^{-1}H \bmod q'} \bmod n = \alpha^1 \bmod n = \alpha.
 \end{aligned}$$

З наведеного вище вираження необхідно, щоб значення двійкового числа K , що відповідає правильності електронного цифрового підпису, можна було обчислити тільки при знанні двійкового числа q' . У той же час таке завдання з використанням тільки відкритого ключа (n , α) розрахунково неможливо здійснити, оскільки для цього необхідно розкласти число n на два більших простих множники, що є практично нерозв'язним завданням.

Для несанкціонованого формування електронного цифрового підпису необхідне знаходження пари багаторозрядних двійкових чисел S і H , при яких справедливе вираження $S \cdot H \bmod n = \alpha$. Однак при великій розрядності числа q' без знання секретного ключа, а саме одного з його складових - двійкового числа q' , це практично неможливо. Цим визначається стійкість системи електронного цифрового підпису, заснованої на способі перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, що заявляється.

Детальне математичне обґрунтування реалізованості стійкості систем електронного цифрового підпису, заснованих на зазначеному вище способі, що заявляється, наведене в [5], [6], [7], [8], [9].

Таким чином, способ перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, що заявляється, може бути покладений в основу стійких систем електронного цифрового підпису, що забезпечують низьку ймовірність несанкціонованого формування електронного цифрового підпису ("помилкового" підтвердження дійсності електронного цифрового підпису).

Наведений приклад і математичне обґрунтування показують, що зазначений спосіб перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, працює коректно, технічно реалізуємо й дозволяє вирішити поставлене завдання. Вся інформація може передаватися по телекомунікаційних мережах і мережах ЕОМ (і може бути використане в державних системах передачі електронних повідомлень (документів), завірених електронним цифровим підписом, включаючи системи передачі даних Збройних Сил України, Міністерства внутрішніх Справ України та Служби безпеки України тощо).

Підвищення ефективності застосування способу перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, який заявляється, у порівнянні з прототипом, полягає в тому, що шляхом зміни процедури формування перевірного багаторозрядного двійкового числа забезпечити зниження ймовірності несанкціонованого

формування електронного цифрового підпису "помилкового" підтвердження дійсності електронного цифрового підпису.

Джерела інформації:

1. Иванов М.А. Криптография. М., КУДИЦ-ОБРАЗ, 2001. - с. 189-191 - аналог.
- 5 2. Молдовян А.А., Молдовян И.А., Советов Б.Я. Криптография. - СПб, Издательство "Лань", 2000. - с. 156-159 - аналог.
3. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. - СПб, Издательство "Лань", 2000. - с. 151-155 - прототип.
- 10 4. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. - СПб, Издательство "БХВ-Петербург", 2004. - С. 95-121.
5. Виноградов И.М. Основы теории чисел. - М.: Наука, 1972. - 167 с.
6. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптографии: скоростные шифры. - СПб, БХВ-Петербург, 2002. - с. 58-61.
- 15 7. Б. Шнайер. Прикладная криптография. - М., изд-во "Триумф", 2002. -с. 278-280.
8. Виноградов И.М. Основы теории чисел. -М.: Наука, 1972. -167 с.;
9. Бухштаб А.А. "Теории чисел". - М.: Просвещение, 1966. – 384 с.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

- 20 1. Спосіб перевірки дійсності електронного цифрового підпису, що завіряє електронний цифровий документ, який полягає в тому, що приймають електронний документ, представлений багаторозрядним двійковим числом N , відкритий ключ у вигляді першого g -розрядного і другого f -розрядного двійкових чисел n і α й електронний цифровий підпис у вигляді багаторозрядного двійкового числа S , формують перевірне багаторозрядне двійкове число V , параметри якого
- 25 порівнюють із параметрами еталонного багаторозрядного двійкового числа, і при їхньому збігу роблять висновок про дійсність електронного цифрового підпису, який **відрізняється** тим, що для формування перевірного багаторозрядного двійкового числа V електронний цифровий підпис підносять до степеня N по модулю, рівному першому g -розрядному двійковому числу n відкритого ключа, при цьому як еталонне багаторозрядне двійкове число використовують друге
- 30 f -розрядне число α відкритого ключа.
2. Спосіб за п. 1, який **відрізняється** тим, що інформацію, яка стосується аутентифікації електронних повідомлень, передають по телекомунікаційних мережах і по мережах ЕОМ, включаючи Internet.

Комп'ютерна верстка Л. Литвиненко

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601