УДК 358.3:528

Міхно О.Г., Камінський В.М.
Київський національний університет імені Тараса Шевченка

ОСОБЛИВОСТІ ШИФРУВАННЯ ГЕОПРОСТОРОВИХ ДАНИХ ДЛЯ ПЕРЕДАВАННЯ ПО ВІДКРИТИХ КАНАЛАХ ЗВ'ЯЗКУ

Ключові слова: *геопросторова інформація, координовані вектори, передавання даних по каналах зв'язку*

Актуальність проблеми. Сучасні бойові дії неможливі без оперативної передачі геопросторових даних між геоінформаційними системами різних ланок збройних сил. Але на відміну від інших різновидів оперативної інформації, геопросторові дані мають деякі особливості, які потрібно враховувати при їх передаванні. Зокрема, до основних типів геопросторової інформації належать:

- растрові зображення;
- цифрово-текстовий опис об'єктів;
- координовані вектори.

Якщо для перших двох типів даних існує велика кількість алгоритмів, які можна застосовувати для їх стиснення (*GIF, JPEG, ZIP, RAR* тощо), то для координованих векторів було б доцільно попередньо трансформувати записи у вигляді зміщення координат. Передавання геопросторових даних по закритих каналах зв'язку на сучасному етапі реформування Збройних Сил України є досить проблематичним, оскільки існуючі закриті канали не забезпечують відповідної продуктивності для таких даних.

Мета статті. Формування алгоритмів шифрування геопросторових даних для передавання відкритими каналами зв'язку.

Виклад основного матеріалу досліджень. Для передавання геопросторових даних по відкритих каналах зв'язку доцільно використовувати алгоритми з відкритим ключем (асиметричні криптосистеми) [1]. В основі їх лежить використання *односторонніх* функцій, тобто функцій, які легко обчислити, але важко обернути. Важке обертання означає, що довільний поліноміальний алгоритм, який буде обертати односторонню функцію, видасть потрібний результат з дуже малою ймовірністю. До відомих односторонніх функцій належать:

1. *Добуток простих чисел* $f(x,y) = xy$. Оберненою до добутку є функція розкладання числа на множники. Сучасним найшвидшим алгоритмом факторизації числа є різновиди квадратичного алгоритму Діксона.
2. *Піднесення до степені за модулем* $f(p,g,x) = g^x \bmod p$. Оберненою є функція обчислення дискретного логарифму: p – просте число, g – генератор

циклічної групи $Z_p^* = (\{x \mid x < p$, НСД $(x, p) = 1\} \bmod p)$:

$$Z_p^* = \{g^i \bmod p \mid 1 \le i \le p - 1\}, \quad g \in Z_p^*.$$

Сучасний найкращий алгоритм обчислення дискретного логарифму базується на обчисленні індексів та має часову оцінку $L(n)^{\sqrt{2}}$ [2]. Відкритою проблемою є пошук генератора g для групи Z_p^* (поліноміальний алгоритм пошуку поки що невідомий).

Розглянемо можливість шифрування геопросторових даних за допомогою добутку простих чисел в криптосистемі RSA (Rivest, Shamir, Adleman) [3]. Перевага такого алгоритму над іншими полягає у відсутності потреби таємно передавати ключ. Алгоритм роботи криптосистеми RSA полягає у наступному (рис.).

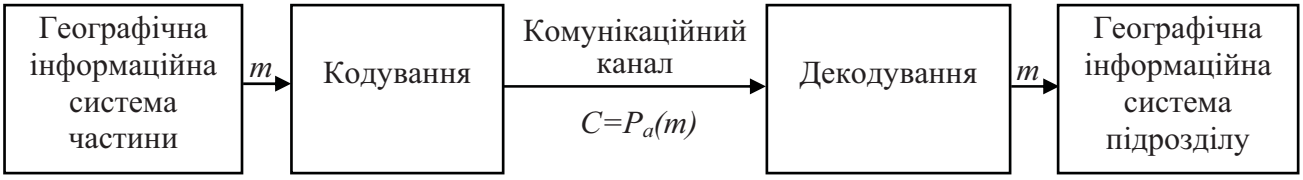

Рис. – **Структурна схема передавання геопросторових даних по відкритому каналу зв'язку**

Кодується повідомлення m за формулою:

$$C = P_a(m) = m^e \bmod n,$$

де, e – довільне натуральне число, взаємно просте з p-1 та q-1, n – добуток двох простих чисел p та q, які залишаються таємними;

Відкритий ключ складається з двох чисел n та e, які передаються по відкритому каналу зв'язку.

Таємний ключ d, за допомогою якого буде декодуватися інформація, обчислюється з рівності $d\ e \bmod ((p\text{-}1)(q\text{-}1)) = 1$, або $d = e^{-1} \bmod ((p\text{-}1)(q\text{-}1))$.

Декодування повідомлення c для отримання повідомлення m проводиться наступним чином:

$$m = c^d \bmod n.$$

Шифрована інформація декодується правильно, оскільки p та q – прості числа, а $\varphi(pq) = \varphi(n) = (p\text{-}1)(q\text{-}1)$, де φ – функція Ейлера. З умови вибору ключа d маємо: $d\ e \bmod \varphi(n) = 1$, або $d\ e = \varphi(n)\ k + 1$ для певного натурального k.

$c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n = m^{\varphi(n)k+1} \bmod n = (m^{\varphi(n)} \bmod n)^k\ m = 1^k\ m = m$, оскільки за теоремою Ейлера $m^{\varphi(n)} \bmod n = 1$.

Закодоване таким чином повідомлення захищене від несанкціонованого доступу настільки, наскільки складно розкласти на множники число n.

Вже відпрацьовані алгоритми для розкладу числа *n* на множники: квадратичне решето, еліптичні криві, метод решета числового поля (general number field sieve) для великих чисел. Вони суттєво не відрізняються за кількістю обчислювальних витрат і можуть бути застосовані для вирішення задачі кодування геопросторової інформації для передавання її по відкритих каналах зв'язку.

Тестування цих алгоритмів показали, що при використанні чисел до 100 знаків, факторизація числа відбувається за декілька хвилин на потужних персональных комп'ютерах. Для факторизації чисел більшого розміру потрібне використання багатопроцесорних систем (тестування проводилось на кластері Київського національного університету імені Тараса Шевченка [3]). При розкладанні чисел розмірністю до 150 десяткових знаків на 44 процесорному кластері з тактовою частотою 2 гГц кожний, процедура факторизації займе більше півроку, а числа розмірністю у 200 десяткових знаків, що знаходяться у конкурсному списку RSA [4], по сьогоднішній день неможливо факторизувати. Тобто, можливо підібрати довжину ключа n, при факторизації якого геопросторова інформація буде вже не актуальна в часі, та який відповідає оперативності – декодування відбувається за короткий термін (декілька мс).

Висновок. Отже передавання геопросторових даних по відкритих каналах зв'язку доцільно робити у два етапи: по-перше, це – стиснення інформації, по-друге, шифрування з відкритим ключем. Причому потрібно розробити ефективні алгоритми для стиснення координовано-векторної інформації (для інших типів даних вже існують ефективні алгоритми) та вибрати відповідну сучасну криптосистему, в якій у відповідності до актуальності даних змінювати довжину ключа n від 120 до 220 десяткових знаків.

Список літератури

1. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. –328 с. **2.** *Lenstra A.K.* Algorithms in number theory / Lenstra A.K, Lenstra H.W.// Handbook of Theoretical Computer Science ; J. van Leeuwen, editor. – Elsevier and MIT Press, 1990. **3.** *Rivest R.L.* A method for obtaining digital signatures and public-key cryptosystems / Rivest R. L., Shamir A., Adleman L.M. // Communications of the ACM. – 1978. – V. 21. – P. 120–126. **4.** http://www.cluster.univ.kiev.ua, **5.** The RSA Challenge Numbers // RSA Laboratories. http://www.rsasecurity.com/rsalabs/node.asp?id=2093/

Особливості шифрування геопросторових даних для передавання по відкритих каналах зв'язку

Міхно О.Г., Камінський В.М.

Проаналізована можливість передавання геопросторових даних по відкритих каналах зв'язку між геоінформаційними системами військового призначення різних рівнів, сформовані вимоги до таких каналів зв'язку.

Ключові слова: геопросторова інформація, координовані вектори, передавання даних по каналах зв'язку.

Особенности шифрования геопространственных данных для передачи по открытым каналам связи

Михно А.Г., Каминский В.Н.

Проанализирована возможность передачи геопространственных данных по открытым каналам связи между геоинформационными системами военного назначения различных уровней, сформированы требования к таким каналам связи.

Ключевые слова: *геопространственная информация, координированные вектора, передача по каналам связи.*

Geospatial information encipherement features for the transmission on the opened communication channels

Mikhno O.G., Kaminskiy V.M.

The possibility of communication of geospatial data on the opened communication channels between the geographic information systems of military destination of different levels is analyzed. The requirement to such channels of connection formed.

Keywords: *geospatial information, coordinated vectors, transmission on connection channels.*

Надійшла до редколегії 09.06.10