УДК 004.056.2

Віталій КАРПІВ, Олег МОМОТЮК, Михайло КАСЯНЧУК

Західноукраїнський національний університет

МАТЕМАТИЧНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЦІЛОЧИСЕЛЬНОГО РОЗЩЕПЛЕННЯ

Вступ. В даний час арифметика в залишках активно застосовується в цифровій обробці сигналів, обробці зображень, у розподілених інфокомунікаційних системах, бездротових сенсорних мережах, засобах забезпечення множинного доступу з кодовим поділом каналів, виявлення та виправлення помилок, у системах інформаційної безпеки, хмарних обчисленнях тощо [1].

Для асиметричної криптографії на операції ділення націло з остачею грунтується переважна більшість відомих методів, зокрема, метод Цезаря, афінна система підстановок Цезаря, метод Хілла, метод Віженера тощо [2].

Однак у цих методах не розглядалося питання багатократного застосування такої операції для кожного символу з метою підвищення рівня безпеки і створення додаткових труднощів для контролю повідомлень, що передаються зі сторони несанкціонованого користувача. Тому тема роботи є актуальною.

Мета: розробити математичну модель захисту інформації на основі цілочисельного розщеплення.

1. Математична модель захисту інформації на основі цілочисельного розщеплення

Нехай дано два додатних цілих числа r і a , для яких виконується нерівність $0<a<r$. Цілочисельним розщепленням числа a за базою r називається подання числа a у вигляді послідовності чисел a_1, a_2, a_3, …, a_{k-1}, a_k, в якій виконуються такі рівності:

$$a_1=\delta^{(2)}, \text{ де } \delta^{(2)}=r \bmod a,$$

$$a_2=\delta^{(3)}, \text{ де } \delta^{(3)}=r \bmod q^{(2)},\ q^{(2)}=\left\lfloor \frac{r}{a} \right\rfloor,$$

$$a_3=\delta^{(4)}, \text{ де } \delta^{(4)}=r \bmod q^{(3)},\ q^{(3)}=\left\lfloor \frac{r}{q^{(2)}} \right\rfloor,$$

$$\ldots\ldots\ldots\ldots \qquad (1)$$

$$a_{k-1}=\delta^{(k)}, \text{ де } \delta^{(k)}=r \bmod q^{(k-1)},\ q^{(k-1)}=\left\lfloor \frac{r}{q^{(k-2)}} \right\rfloor,$$

$$a_k=q^{(k)}, \text{ де } q^{(k)}=\left\lfloor \frac{r}{q^{(k-1)}} \right\rfloor,$$

де $\delta^{(2)}$ – залишок при цілочисельному діленні r на a, а $q^{(i)}$ – ціла частина при такому діленні; $\delta^{(i)}$ – залишок при цілочисельному діленні r на $q^{(i-1)}$; символ $\lfloor\ \rfloor$ означає округлення до найближчого цілого в меншу сторону.

Натуральне число k називається рівнем розщеплення. Цілочисельне розщеплення є певним узагальненням математичної операції ділення із залишком.

Блок-схема цілочисельного розщеплення числа a за базою r при рівні розщеплення k показана на рисунку 1.

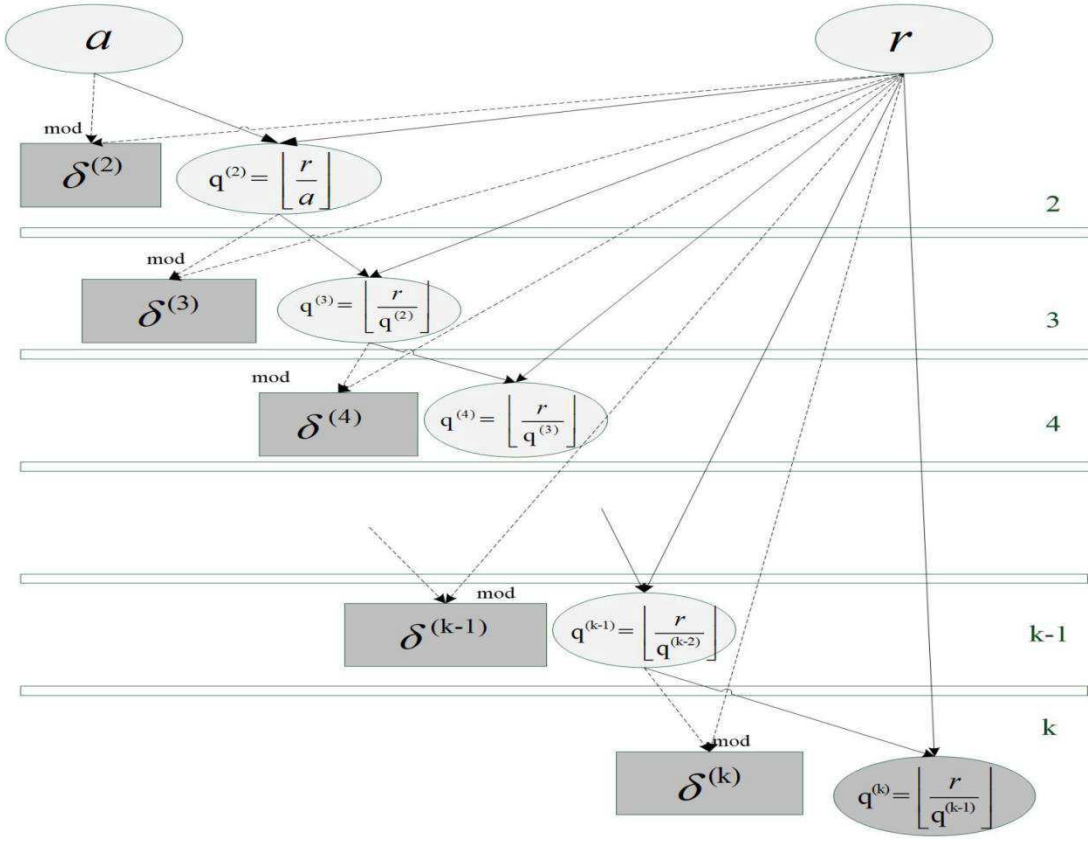

Рисунок 1 - Блок-схема цілочисельного розщеплення числа a за базою r при рівні розщеплення k

Функцією відображення $\Phi_k(a, r)$ називається результат цілочисельного розщеплення числа a за основою r.

Відповідно до (1), функція відображення $\Phi_k(a, r)$ при рівні розщеплення, що дорівнює k, задається наступним співвідношенням:

$$\Phi_k(a, r)=(\delta_a^{(2)}, \delta_a^{(3)}, \delta_a^{(4)}, \ldots, \delta_a^{(k-1)}, \delta_a^{(k)}, q_a^{(k)}). \quad (2)$$

Наприклад, відображення $\Phi_k(a, r)$ при рівні розщеплення k=3 визначається наступним співвідношенням:

$$\Phi_3(a, r)=(\delta_a^{(2)}, \delta_a^{(3)}, q_a^{(3)}).$$

2. Розщеплення по векторній базі

Усі теореми допускають природне узагальнення, зв'язане з динамікою у застосунках. Зокрема, можна розглядати узагальнене розщеплення рівня k за векторною базою. Розщеплення по векторній базі - це узагальнене розщеплення рівня k по векторній базі $\vec{r} = (r_1, r_2, ..., r_l)$. Причому черговий ($i$-ий) крок процесу цілочисельного розщеплення виконується щоразу при новому значенні бази розщеплення.

Узагальненим цілим розщепленням числа a по векторній базі

$$\vec{r} = (r_1, r_2, ..., r_l),\ l=k\text{-}1,$$

називається подання числа a у вигляді послідовності цілих чисел a_1, a_2, a_3, …, a_{k-1}, a_k, у якій:

$$a_1=\delta^{(2)},\ \text{де}\ \delta^{(2)}=r_1 \bmod a,\ r_1>a,$$

$$a_2=\delta^{(3)},\ \text{де}\ \delta^{(3)}=r_2 \bmod q^{(2)},\ q^{(2)}=\left\lfloor \frac{r_1}{a} \right\rfloor,\ r_2>q^{(2)},$$

$$a_3=\delta^{(4)},\ \text{де}\ \delta^{(4)}=r_3 \bmod q^{(3)},\ q^{(3)}=\left\lfloor \frac{r_2}{q^{(2)}} \right\rfloor,\ r_3>q^{(3)},$$

$$\ldots\ldots\ldots\ldots \qquad (3)$$

$$a_{k-1}=\delta^{(k)},\ \text{де}\ \delta^{(k)}=r_{k-1} \bmod q^{(k-1)},\ q^{(k-1)}=\left\lfloor \frac{r_{k-2}}{q^{(k-2)}} \right\rfloor,\ r_{k-1}>q^{(k-1)},$$

$$a_k=q^{(k)},\ \text{де}\ q^{(k)}=\left\lfloor \frac{r_{k-1}}{q^{(k-1)}} \right\rfloor.$$

Тут символи $\delta^{(i)}$ позначають залишки при цілочисельному діленні r_i на $q^{(i)}$. Це визначення є узагальненням схеми математичного цілочисельного розщеплення. Таке розщеплення виявляється найбільш корисним у застосунках, пов'язаних із захистом інформації, що передається.

Є багато способів, які можуть бути виконані для перевірки правильності вилучення відкритого тексту із зашифрованого з використанням процедури узагальненого розщеплення на стороні одержувача.

Один із цих способів, в яких обробляється символ за символом, можна пояснити так:

1) якщо значення перевіряє умову $r_i>q^{(i)}$, де i=2, 3, …, k-1, тобто використовують його у процесі шифрування;

2) якщо значення r_i не перевіряє умову $r_i>q^{(i)}$, де i=2, 3, …, k-1, то в процесі шифрування виконуються такі кроки:

- пропустити поточне значення ri і використовувати наступне значення ri+1 у згенерованій послідовності гам;
- додати 0 ліворуч від результату залишку, який буде розрахований з використанням гами r_{i+1} (функція цього 0 не змінить значення залишку, але в процесі отримання відкритого тексту повідомить одержувача зашифрованого тексту про те, що в послідовності гам є невикористане пропущене значення r_i.

Передбачається, що зв'язок безшумний, тобто у каналі зв'язку відсутні перешкоди. Однак наявність перешкод можна грубо оцінити теоретично при передачі замість символу його розщеплення. У цій роботі буде всюди передбачатися, що канал зв'язку є безшумним, як і у випадку передачі даних між двома комп'ютерами виділеної лінії.

Висновок. Розроблено математичну модель захисту інформації на основі цілочисельного розщеплення.

Перелік використаних джерел.

1. Samuel S., Wagstaff Jr. Cryptanalysis of Number Theoretic Ciphers. RC Press, 2019. 336c.

2. Rubin F. Secret Key Cryptography: Ciphers, from Simple to Unbreakable. Manning, 2022. 344c.