КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 9

Математические основы криптографии: решение сравнений первой степени с одним неизвестным

Данный материал демонстрирует разбор задания, посвященного решению сравнений первой степени с одним неизвестным.

Сравнением первой степени с одним неизвестным называется сравнение вида $ax = b \pmod m$, где x является неизвестным.

Сравнения в кольце целых чисел равносильны уравнениям в кольце классов вычетов по соответствующему модулю.

Существует три возможных случая решения сравнения первой степени с одним неизвестным:

- если $\text{НОД}(a, m) = 1$, то множеством решений является класс вычетов $a^{-1} \cdot b \in \mathbb{Z}_m$;
- если $\text{НОД}(a, m) = \text{d} > 1$ и $d \nmid b$, то решений не существует;
- если $\text{НОД}(a, m) = \text{d} > 1$ и $d|b$, то множеством решений являются d классов вычетов по модулю m, образующих один класс вычетов по модулю d: $\tilde{a}^{-1} \cdot \tilde{b} \in \mathbb{Z}_{\tilde{m}}$; $\left(\tilde{a}^{-1} \cdot \tilde{b} + \tilde{m}\right) \in \mathbb{Z}_{\tilde{m}}$; …, $\left(\tilde{a}^{-1} \cdot \tilde{b} + \tilde{m}(d-1)\right) \in \mathbb{Z}_{\tilde{m}}$.

В том случае, если сравнение первой степени с одним неизвестным имеет решение, для его нахождения необходимо вычислить $a^{-1} \pmod m$ (или же $\tilde{a}^{-1} \pmod{\tilde{m}}$). Для этого необходимо использовать расширенный алгоритм Евклида.

Пример.

Решить сравнение $112x \equiv 9 \pmod{423}$.

Решение.

Сначала необходимо определить, какому из трех возможных случаев соответствует данное сравнение первой степени с одним неизвестным. Для этого найдем наибольший общий делитель чисел 112 и 423. В общем случае для этого целесообразно воспользоваться расширенным алгоритмом Евклида. Можно ограничиться алгоритмом Евклида, однако если $\text{НОД}(112, 423)$ окажется равным единице, то для дальнейшего решения понадобится $112^{-1} \pmod{423}$, поэтому лучше использовать расширенный алгоритм.

Соответствующие вычисления приведены в таблице ниже.

q	r	x	y	a	b	x_2	x_1	y_2	y_1
—	—	—	—	423	112	1	0	0	1
3	87	1	–3	112	87	0	1	1	–3
1	25	–1	4	87	25	1	–1	–3	4
3	12	4	–15	25	12	–1	4	4	–15
2	1	–9	34	12	1	4	–9	–15	34
12	0	112	–423	1	0	–9	112	34	–423

Из таблицы следует, что $\text{НОД}(112, 423) = 1$. Следовательно, данное сравнение относится к первому случаю, когда множеством решений является класс вычетов $a^{-1} \cdot b \in \mathbb{Z}_m$. Из этой же таблицы следует, что $112^{-1} \pmod{423} = 34$.

Тогда $x = 34 \cdot 9 \pmod{423} = 306$.

Если подставить полученное значение в исходное выражение, то можно убедиться, что оно действительно является решением данного сравнения первой степени с одним неизвестным:

$112 \cdot 306 = 34272 = 9 \pmod{423}$.