Теория чисел в криптографии

14 апреля 2019 г., АНО Школа 21

Важные определения

Наибольшим общим делителем двух целых чисел a и b, одновременно не равных нулю, называется такое наибольшее целое число d, на которое a и b делятся без остатка.

Основная теорема арифметики

Каждое натуральное число $n > 1$ можно представить в виде $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$, где p_n - простые числа, причем такое представление единственно с точностью до перестановки.

Малая теорема Ферма

Если $a \in \mathbb{Z}$ не делится на простое число p, то $a^{p-1} \equiv 1 (mod\ p)$.
Данная теорема лежит в основе теста простоты Ферма.

1. Докажите, что если $a \equiv b (\text{mod } m)$ и $c \equiv d (\text{mod } m)$, то
   (a) $a + c \equiv b + d \ (\text{mod } m)$;
   (b) $a \cdot c \equiv b \cdot d \ (\text{mod } m)$.
2. Найти наибольший общий делитель чисел $2^n - 1$ и $2^m - 1$, где $n, m \in \mathbb{N}$
3. Докажите, что:
   (a) $\varphi(m^2) = m \cdot \varphi(m) \ \forall m \in \mathbb{N}$;
   (b) $\varphi(m^k) = m^{k-1} \cdot \varphi(m) \ \forall m, k \in \mathbb{N}$.
4. Доказать, что если $n \in \mathbb{N}$ составное, то хотя бы один простой делитель n лежит на промежутке $[2; \lfloor \sqrt{n} \rfloor]$.
5. Применить тест Ферма для проверки на простоту чисел 511 и 509.

Алгоритм Шифрования RSA (Rivest, Shamir и Adleman)

1. *Сформировать "модуль" $n = p \cdot q$, p и q - большие простые числа.*
2. *Посчитать $\varphi(n)$.*
3. *Выбрать "Открытую Экспоненту" e, такую что $1 < e < \varphi(n), (e, \varphi(n)) = 1$.*
4. *Выбрать "закрытую экспоненту" d, такую что $d \cdot e - 1 \vdots \varphi(n)$.*
5. *Опубликовать пару (e, n).*
6. *Отправляющая сторона шифрует сообщение m:$E(m) = m^e \mod n$.*
7. *Принимающая сторона расшифровывает принятое сообщение m': $D(m') = m'^d \mod n$.*

Теория чисел в криптографии

14 апреля 2019 г., АНО Школа 21

Важные определения

Наибольшим общим делителем двух целых чисел a и b, одновременно не равных нулю, называется такое наибольшее целое число d, на которое a и b делятся без остатка.

Основная теорема арифметики

Каждое натуральное число $n > 1$ можно представить в виде $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$, где p_n - простые числа, причем такое представление единственно с точностью до перестановки.

Малая теорема Ферма

Если $a \in \mathbb{Z}$ не делится на простое число p, то $a^{p-1} \equiv 1 (mod\ p)$.
Данная теорема лежит в основе теста простоты Ферма.

1. Докажите, что если $a \equiv b (\mathrm{mod}\ m)$ и $c \equiv d (\mathrm{mod}\ m)$, то
   (a) $a + c \equiv b + d\ (\mathrm{mod}\ m)$;
   (b) $a \cdot c \equiv b \cdot d\ (\mathrm{mod}\ m)$.
2. Найти наибольший общий делитель чисел $2^n - 1$ и $2^m - 1$, где $n, m \in \mathbb{N}$
3. Докажите, что:
   (a) $\varphi(m^2) = m \cdot \varphi(m)\ \forall m \in \mathbb{N}$;
   (b) $\varphi(m^k) = m^{k-1} \cdot \varphi(m)\ \forall m, k \in \mathbb{N}$.
4. Доказать, что если $n \in \mathbb{N}$ составное, то хотя бы один простой делитель n лежит на промежутке $[2; \lfloor\sqrt{n}\rfloor]$.
5. Применить тест Ферма для проверки на простоту чисел 511 и 509.

Алгоритм Шифрования RSA (Rivest, Shamir и Adleman)

1. *Сформировать "модуль" $n = p \cdot q$, p и q - большие простые числа.*
2. *Посчитать $\varphi(n)$.*
3. *Выбрать "Открытую Экспоненту" e, такую что $1 < e < \varphi(n), (e, \varphi(n)) = 1$.*
4. *Выбрать "закрытую экспоненту" d, такую что $d \cdot e - 1 \vdots \varphi(n)$.*
5. *Опубликовать пару (e, n).*
6. *Отправляющая сторона шифрует сообщение m:$E(m) = m^e \mod n$.*
7. *Принимающая сторона расшифровывает принятое сообщение m': $D(m') = m'^d \mod n$.*