14 Криптосистемы с открытыми ключами

Функция Эйлера $\varphi(n)$ — число натуральных чисел $m \leq n$ взаимно простых с n. Если число n имеет каноническое разложение $n = p_1^{s_1} \cdot \ldots p_k^{s_k}$, то справедлива формула

$$\varphi(n) = n \cdot \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Теорема (Эйлер). Если натуральные числа x и n взаимно просты, то выполняется

$$x^{\varphi(n)} \equiv 1 (\operatorname{mod} n).$$

Теорема (китайская теорема об остатках). Если натуральные числа $m_1, m_2, \ldots, m_k$ попарно взаимно просты, то система сравнений

$$x \equiv a_1 (\operatorname{mod} m_1),\ x \equiv a_2 (\operatorname{mod} m_2),\ \ldots,\ x \equiv a_k (\operatorname{mod} m_k)$$

имеет единственное решение по модулю $n = m_1 m_2 \ldots m_k$ при любых целых числах $a_1, a_2, \ldots, a_k$.

14.1 Найти дискретный логарифм числа 7 по основанию 2 в группе $\mathbb{Z}/19\mathbb{Z}$.

14.2 Пусть поле $GF(3^2)$ построено с помощью неприводимого многочлена $x^2 - x - 1$. Найти дискретный логарифм по основанию x элемента поля -1.

14.3 Пусть известен открытый ключ $p = 23$. Каким образом Алиса может передать Бобу секретное сообщение $m = 17$?

14.4 Для получения секретной информации используется криптосистема RSA. Выбрав два простых числа p и q, Алиса формирует число $n = p \cdot q$ и выбирает e взаимно простым с числом $\varphi(n)$. Затем она публикует пару $\{n, e\}$ в газете "Университетская жизнь". Используя открытый ключ, передать Алисе секретное сообщение m. Дешифровать его с помощью секретного ключа.

а) $p = 11$, $q = 17$, $e = 9$, $m = 3$;
б) $p = 17$, $q = 31$, $e = 7$, $m = 2$.

14.5 Для электронной подписи используется криптосистема RSA. Секретный ключ банкира Боба составляют числа $\{p_B, q_B\}$, а секретный ключ вкладчика Алисы — числа $\{p_A, q_A\}$. Пусть открытыми ключами Боба и Алисы являются пары $\{n_B = p_B \cdot q_B, e_B\}$ и $\{n_A = p_A \cdot q_A, e_A\}$ соответственно, где $(e_B, \varphi(n_B)) = (e_A, \varphi(n_A)) = 1$. Нужно передать Бобу секретное поручение m от Алисы.

а) $p_A = 11, q_A = 23, e_A = 31$, $p_B = 7, q_B = 13, e_B = 5$, $m = 41$.

Семинар 15 Коллоквиум по сжатию и криптографии.