ДМ-2. Задачі до лекції 9.

Теорія чисел і криптографія: криптосистеми з відкритим ключем; криптографічні протоколи

Довідковий матеріал

Таблиця 1.

Латинська абетка

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Таблиця 2.

Українська абетка

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И
0	1	2	3	4	5	6	7	8	9	10
І	Ї	Й	К	Л	М	Н	О	П	Р	С
11	12	13	14	15	16	17	18	19	20	21
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
22	23	24	25	26	27	28	29	30	31	32

Задачі

1. Зашифрувати повідомлення UPLOAD з використанням системи RSA з $n = 53 \cdot 61$ та $e = 17$. Замінити кожну букву парою цифр і згрупувати пари цілих чисел, як це було зроблено в прикладі лекції 9.

2. Зашифрувати повідомлення ЗУСТРІЧ НЕ ВІДБУЛАСЯ з використанням системи RSA з $n = 53 \cdot 67$ та $e = 17$. Замінити кожну букву парою цифр і згрупувати пари цілих чисел, як це було зроблено в прикладі лекції 9.

3. Дешифрувати повідомлення, яке було зашифроване з використанням системи RSA з $n = 53 \cdot 61$ та $e = 17$, якщо зашифроване повідомлення таке: 3185 2038 2460 2550. (Для розшифрування спочатку знайдіть дешифрувальну експоненту d, яка є оберненою до $e = 17$ за модулем $52 \cdot 60$.)

4. Дешифрувати повідомлення, яке було зашифроване з використанням системи RSA з $n = 43 \cdot 59$ та $e = 13$, якщо зашифроване повідомлення таке: 0667 1947 0671. (Для розшифрування спочатку знайдіть дешифрувальну експоненту d, яка є оберненою до $e = 13$ за модулем $42 \cdot 58$.)

5. Дешифрувати повідомлення, яке було зашифроване з використанням системи RSA з $n = 53 \cdot 67$ та $e = 17$, якщо зашифроване повідомлення таке: 3153 2335. (Для розшифрування спочатку знайдіть дешифрувальну експоненту d, яка є оберненою до $e = 13$ за модулем $52 \cdot 66$.)

6. Описати кроки, які мають виконати Аліса і Боб для реалізації протоколу обміну для генерування секретного ключа. Припустімо, що вони використовують просте число $p = 23$ і взяли $a = 5$, що є примітивним коренем 23. Нехай Аліса вибрала $k_1 = 8$, а Боб вибрав $k_2 = 5$.

7. Описати кроки, які мають виконати Аліса і Боб для реалізації протоколу обміну для генерування секретного ключа. Припустімо, що вони використовують просте число $p = 101$ і взяли $a = 2$, що є примітивним коренем 101. Нехай Аліса вибрала $k_1 = 7$, а Боб вибрав $k_2 = 9$.

8. Аліса хоче розіслати всім своїм друзям, включно з Бобом, повідомлення «SELL EVERYTHING» так, щоб усі вони були впевнені, що лист надійшов саме від неї. Що саме має надіслати їм Аліса, якщо має бути використана система RSA? Параметри: $n = 61 \cdot 47 = 2867$ і $e = 7$. Секретний ключ d обчислюють як обернене до $e = 7$ за модулем $60 \cdot 46 = 2760$, за допомогою Modular Arithmetic Calculator знаходимо $d = 1183$.