ЗАДАЧИ ПО КРИПТОГРАФИЯ – ФМИ, 2020

1. Да се дешифрира криптотекста

   `EB QX ZL HD LK IV QG OM AL EB VB DO SG SF`

   `ZR AN DA MO LB SE EL SO ZL KD CO ZF GS IN`

   ако е известно, че е използван шифър на Playfair, при който

   `THEWINTEROFOURDISCONTENT.`

   се шифрира в

   `WGNZDZWNISOSBHGRREAZWNTW.`

2. Често се приема за полезно шифриращата и дешифриращата трансформации да съвпадат. В случая на шифъра на Хил това означава $K = K^{-1}$. Да се определи броя на матриците от ред 2 над $\mathbb{Z}_{26}$, за които това е изпълнено.

3. Да се намери ключа на шифър на Хил, който шифрира съобщението `CRYPTOGRAPHY` в `VGYXARDIGLML`. Дължината на ключа е неизвестна (но може да допуснем, че дели дължината на шифрираното съобщение). Използвана е схемата за кодиране `A`$\rightarrow 0$,`B`$\rightarrow 1$,`C`$\rightarrow 2$ и т.н. до `X`$\rightarrow 23$,`Y`$\rightarrow 24$,`Z`$\rightarrow 25$.

4. Известно е, че за обмен на данни е използвана системата "Автоключ" с дължина на ключовата дума $m = 6$. Да се декодира криптотекстът:

   `GXILB GLQQJ AIPWB MRKAZ BWYKK KUCRKG`

   ако е известно, че откритият текст съдържа думата `GESTURE`. (Може да напишете малка програма.)

5. Изпозван е пермутационен шифър грид с размер 6×6, имащ 5 забранени полета, чиято позиция е неизвестна. Да се направи криптанализ на съобщението

   `ACAUI MMGRC AILEE HKREG EAISW OSTHDS .`

6. Да се построи линеен регистър, пораждащ двоична редица с перид 21.

7. Да разгледаме небалансиран шифър на Файстел. При него всеки блок открит текст е с дължина $m+n$ и се разбива на два подблока: A с дължина m и B – с дължина n. Шифрирането се състои от h еднотипни стъпки. На i-тата стъпка (A, B) се преобразува в (A', B'), където A' е с дъжина n, а B' с дължина m по правилото:

   $$\begin{aligned} A' &= B \\ B' &= A \oplus f_i(B) \end{aligned}$$

   Да се шифрира блока 101101, ако е използван небалансиран Файстел с $m = 2, n = 4$, $h = 4$ и трансформации $f_1, \ldots, f_4$, зададени чрез

	0000	0001	0010	0011	0100	0101	0110	0111
f_1	00	10	11	11	01	01	01	10
f_2	10	11	00	11	10	11	01	01
f_3	10	00	00	01	01	10	10	11
f_4	11	10	01	10	00	10	00	00

	1000	1001	1010	1011	1100	1101	1110	1111
f_1	10	01	10	11	00	00	00	00
f_2	01	11	10	00	10	11	01	00
f_3	01	11	00	10	11	10	11	01
f_4	10	01	00	10	01	11	10	11

8. Дадена е криптосистема RSA с модул $n = pq$ и шифрираща експонента e. Докажете, че броят на откритите текстове m, които се шифрират в себе си, т.е. за които $m^e \equiv m \pmod{n}$, е

$$(1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1)).$$

9. Намерете чрез алгоритъма на Pohlig-Hellman $\log_2 66$ в $\mathbb{Z}_{101}^*$.

10. Нека $n = pq$, където p и q са прости числа. Известен е алгоритъм $\mathcal{A}$, който намира решение на сравнението $x^2 \equiv c \pmod{n}$ в $F(n)$ стъпки за всяко c, което е квадрат на елемент от $\mathbb{Z}_n$. Да се докаже, че съществува вероятностен алгоритъм, който разлага n в (очакван брой) $2(F(n) + 2\log_2 n)$ стъпки.

11. Потребителите A и B използват схемата на Diffie и Hellman, използваща дискретен логаритъм за да уговорят таен ключ. Те използват крайното поле $GF(2^{10}) = \mathbb{F}_2[x]/(x^{10}+x^3+1)$. Потребителят B публикува низа $c_B = 0100010100$, който представя елемента $x+x^5+x^7$ от $GF(2^{10}) = \mathbb{F}_2[x]/(x^{10}+x^3+1)$. Ако тайният ключ на A е $x_A = 2$, какъв ключът, който A и B ще използват при комуникацията помежду си?

12. Дадени са простото число $p = 101$, примитивният елемент $\alpha = 2$ и $x_U = 43$. Използвайки схемата на ElGamal, намерете валиден подпис за съобщението $m = 26$. Проверете валидността на генерирания подпис.

13. Да се пресметне $\log_3 135$ в полето $\mathbb{Z}_{353}^*$.

14. Дадени са свръх нарастващият вектор $\boldsymbol{a} = (2, 3, 7, 13, 27, 53, 106, 213, 425, 851)$, модулът $m = 1529$ и $t = 64$. Шифрирайте съобщението `LONDON`. Използвайте кодирането

A	00011	H	01100	O	10100	V	11011
B	00101	I	01101	P	10101	W	11100
C	00110	J	01110	Q	10110	X	11101
D	00111	K	01111	R	10111	Y	11110
E	01001	L	10001	S	11000	Z	11111
F	01010	M	10010	T	11001		
G	01011	N	10011	U	11010		

15. В общия случай е неизвестно дали задачата за криптанализ на RSA с експонента $e = 3$ е еквивалентна на разлагането на модула n на RSA. При създаване на този вариант на RSA трябва да осигурим, че 3 не дели $\varphi(n)$. В тази задача изследваме случая, когато 3 дели $\varphi(n)$. Да разгледаме $n = pq$, където p и q са нечетни прости числа.

    (i) При какво условие за p и q е вярно, че 3 дели $\varphi(n)$?

    (ii) Елементът $x \in \mathbb{Z}_n^*$ се нарича кубичен остатък по модул n, ако съществува елемент $y \in \mathbb{Z}_n^*$, такъв, че $y^3 \equiv x \pmod{n}$. Нека C_n е множеството на всички кубични остатъци от $\mathbb{Z}_n*$.

    • Нека $x \in C_n$. Какъв е броят на кубичните корени, когато $p \equiv 1 \pmod{3}$ и $q \equiv 2 \pmod{3}$?

    • Какъв е броят на кубичните корени, когато $p \equiv q \equiv 1 \pmod{3}$.

    • Да допуснем, че 3 дели $\varphi(n)$. Нека са известни два различни кубични корена y и z на даден елемент $x \in C_n$. Как може да се намери разлагането на n от $y - z$. Оценете вероятността за успех.

(iii) Отново да допуснем, че 3 дели $\varphi(n)$ и да приемем, че разполагаме с оракул, който при даден кубичен остатък $x \in C_n$ връща един кубичен корен на x, да речем y. Докажете, че този кубичен корен може да се използва за да се намери разлагането на n. Оттук докажете, че проблемът за криптанализ на RSA с $e = 3$ е еквивалентен на разлагането на n. (NB. Това доказателство е валидно само когато 3 дели e.)

16. Нека $n = pq$, където p и q са прости числа. Намерете корените на уравнението $x^2 - ax + n = 0$, където $a = n + 1 - \varphi(n)$. Намерете тези корени в явен вид и обяснете, как може да се намерят p и q с помощта на прост алгоритъм за намиране на квадратен корен. Намерете разлагането на n при $n = 15049$, $\varphi(n) = 14800$.

17. Нека p е просто число и нека G е множеството на всички елементи $x \in \mathbb{Z}_{p^2}$, удовлетворяващи $x \equiv 1 \pmod{p}$.

    (i) Докажете, че G е група по отношение умножението в $\mathbb{Z}_{p^2}$.

    (ii) Докажете, че $|G| = p$.

    (iii) Докажете, че $L : G \to \mathbb{Z}_p$, зададено с $L(x) = \frac{x-1}{p} \pmod{p}$ е изоморфизъм на групи.

    (iv) Докажете, че $p + 1$ е пораждащ елемент на G и че изоморфизмът L е дискретен логаритъм при основа $p + 1$ в G. С други думи $(p + 1)^{L(x)} \pmod{p^2} = x$ за всяко x.

18. **Криптосистема на Окамото-Учияма.**

    Генериране на ключове. Избираме две големи прости числа p и q, надхвърлящи 2^k за някакво фиксирано k, и пресмятаме $n = p^2 q$. Избираме случайно $g \in \mathbb{Z}_n^*$ такова, че $g^{p-1} \pmod{p^2}$ е от (мултипликативен) ред p. Пресмятаме $h = g^n \pmod{n}$. Публичният ключ е (n, g, h); тайният ключ е (p, q).

    Шифриране. Откритият текст е число $m \in \mathbb{N}$, за което $0 < m < 2^{k-1}$. Избираме случайно $r \in \mathbb{Z}_n^*$. Криптотекстът, съответстващ на m, се задава със $c = g^m h^r \pmod{n}$.

    Дешифриране. Откритият текст m се получава от равенството

    $$m = \frac{L(c^{p-1} \pmod{p^2})}{L(g^{p-1} \pmod{p^2})} \pmod{p}.$$

    Да се докаже, че дешифрирането е дефинирано коректно (т.е. че $L(c^{p-1} \pmod{p^2})$ и $L(g^{p-1} \pmod{p^2})$ са наистина елементи на $\mathbb{Z}_p^*$) и че то наистина възстановява оригиналния текст.

19. Нека две партии, да речем Алис и Боб, използват RSA с един и същ модул n, но с различни (публични) шифриращи експоненти e_1 и e_2.

    (i) Докажете, че Алис може да дешифрира съобщения, изпратени до Боб.

    (ii) Докажете, че криптаналаист може да дешифрира съобщение, изпратено едновременно до Алис и до Боб, при условие, че $\gcd(e_1, e_2) = 1$.

20. **Криптосистема на Рабин.**

    Генериране на ключове. Генерираме две големи прости числа p и q, $p \equiv q \equiv 3 \pmod{4}$. Полагаме $n = pq$ и избираме случаен елемент $B \in \mathbb{Z}_n$. Публичен ключ е двойката (B, n), а таен ключ – двойката (p, q).

    Шифриране. Съобщение $x \in \mathbb{Z}_n$ се шифрира като $E(x) = x(x + b) \pmod{n}$.

    Дешифриране. Нека $y \in \mathbb{Z}_n$ е криптотекст. Дешифрираният открит текст $D(y)$ е една от четирите стойности

    $$\sqrt{\frac{B^2}{4} + y} - \frac{B}{2}.$$

    (Имаме четири квадратни корена по модул $n = pq$.)

(i) Как можем да пресмятаме ефективно квадратни корени в $\mathbb{Z}_n$?

(ii) Дешифрирането в така описната система не е определено еднозначно. Покажете, че то може да бъде направено еднозначно като добавим известен излишък в открития текст.

(iii) Докажете, че ако разполагаме с алгоритъм за разлагане на n на прости множители, то можем ефективно да разбием системата на Рабин.

(iv) Докажете, че системата на Рабин може да бъде разбита чрез атака с избран криптотекст (chosen ciphertext attack).

21. **Криптосистема на Naccache-Stern.**

Генериране на ключове. Нека $n = pq$, където $p = 2au+1$, $q = 2bv+1$; a и b са също големи различни прости числа, а u и v се избират както следва. Разглеждадме 10 малки (около 10 бита) нечетни различни прости числа $r_1, \ldots, r_{10}$ и полагаме $u = \prod_{i=1}^{5} r_i$, $q = \prod_{i=6}^{10} r_i$. Полагаме също $\sigma = uv$. Нека $g \in \mathbb{Z}_n^*$ е елемнт, който поражда подгрупа от ред кратен на σab. Публичен ключ е двойката (n, g); таен ключ е двойката (p, q). (Числата a, b, r_i могат да бъдат получени лесно от p и q, така че те имплицитно се включват в тайния ключ.)

Шифриране. Нека $m \in \{1, \ldots, \sigma\}$. Шифрираме m като пресметнем $c = g^m \pmod{n}$. (Тъй като шифриращата страна не разполага със σ, тя използва открити текстове, които са по-малки от някаква долна граница за σ.)

(i) Оценете сигурността на системата в случая когато $a = b = 1$.

(ii) Докажете, че редът на най-голямата циклична подгрупа на $\mathbb{Z}_n^*$ е $2ab\sigma$.

(iii) Нека H е комутативна група от ред t, $t = cd$, където c е просто число, а d е цяло число, което не се дели на p. Нека $h \in H$. Докажете, че ако $h^d \neq 1$, то редът на h е кратен на c.

(iv) Предложете алгоритъм, който проверява дали даден елемент $g \in \mathbb{Z}_n^*$ е от ред поне σab.

(v) Докажете, че шифриращата функция, дефинирана върху $\{1, \ldots, \sigma\} \subset \mathbb{N}$, е инективна.

(vi) Покажете как можем да възстановим съобщението m от криптотекста $c = g^m \pmod{n}$ (Тъй като дешифрирането се извършва от законния получател, то може да бъде използван тайния ключ).

Упътване. Адаптирайте алгоритъма на Полиг-Хелман.

22. Нека C е двоичен линеен $[9, 4, 4]$-код с пораждаща матрица

$$g = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Първите осем координати са асоциитрани съответно с потребителите U_1 до U_8, а последната координата е асоциирана с дилъра D. Да се опише структурата на достъп, реализирана от този код. (Достатъчно е да се опишат минималните авторизирани множества.)

София, 15.04.2020 г.