ЗАДАЧИ ПО КРИПТОГРАФИЯ

1. Даден е шифър на Playfair с ключ

H	O	W	M	A
N	Y	E	L	K
S	B	C	D	F
G	I/J	P	Q	R
T	U	V	X	Z

Шифрирайте текста: APATIENTBETTERDRIVER.

Дешифрирайте криптотекста: BRUTVNGAKWUGOGKPAWPKQGMBVBUGWC.

2. Даден е криптотекстът QCPTKZ, получен чрез шифриране с шифър на L. Hill с ключ

$$\begin{pmatrix} 5 & 2 & 2 \\ 2 & 5 & 2 \\ 2 & 2 & 5 \end{pmatrix}$$

Дешифрирайте, ако е известно, че е използвано кодирането A$\to$ 0, B$\to$ 1, C$\to$ 2 и т.н. X$\to$ 23, Y$\to$ 24, Z$\to$ 25.

3. Да се намери минималният възможен период на линейна рекурентна редица над $GF(2)$, удовлетворяваща рекурентното уравнение

$$a_{n+7} = a_{n+6} + a_{n+5} + a_{n+1} + a_n$$

и имаща ненулево начално състояние.

4. Даден е шифър на Feistel с $n = 2$ и $h = 6$. Ключът k е избран така, че

$$f_{k_1} = \begin{pmatrix} 00 & 01 & 10 & 11 \\ 10 & 10 & 00 & 01 \end{pmatrix}, f_{k_2} = \begin{pmatrix} 00 & 01 & 10 & 11 \\ 01 & 10 & 10 & 00 \end{pmatrix},$$

$$f_{k_3} = \begin{pmatrix} 00 & 01 & 10 & 11 \\ 11 & 00 & 01 & 10 \end{pmatrix}, f_{k_4} = \begin{pmatrix} 00 & 01 & 10 & 11 \\ 11 & 10 & 11 & 01 \end{pmatrix},$$

$$f_{k_5} = \begin{pmatrix} 00 & 01 & 10 & 11 \\ 11 & 00 & 00 & 10 \end{pmatrix}, f_{k_6} = \begin{pmatrix} 00 & 01 & 10 & 11 \\ 11 & 11 & 01 & 10 \end{pmatrix}.$$

Шифрирайте съобщението $m = (0100)$. Дешифрирайте за да се убедите в коректността на шифрирането.

5. Да се построи линеен регистър с минимална дължина, генериращ редицата $(a_i)_{i=0}^{9} = (0110000111)$.

6. Да означим с $DES_K(x)$ образа на 64-битовия блок x при трансформация с DES с ключ K. Докажете, че за всяко $K \in \{0,1\}^{56}$ и всяко $x \in \{0,1\}^{64}$ е в сила

$$DES_k(x) = \overline{DES_{\overline{K}}(\overline{x})}.$$

Как може да се експлоатира това свойство за ускоряване на пълното изчерпване на ключовете при криптанализ с известен открит текст.

7. Дадена е RSA с параметри $n = 899$, $e = 611$. Разложете n на прости множители и пресметнете d. Дешифрирайте криптотекста 106 680 303, като имате пред вид, че при шифрирането буквите от открития текста са преобразувани по следното правило: на всяка двойка букви xy е съпоставено числото $\alpha(x) + 26\alpha(y)$, където $\alpha(A) = 0, \alpha(B) = 0, \alpha(C) = 2, \ldots, \alpha(X) = 23, \alpha(Y) = 24, \alpha(Z) = 25$.

8. Да се докаже, че съществуват безбройно много съставни числа n, за които е изпълнено:
   (a) $2^{n-1} \equiv 1 \pmod{n}$; (b) $3^{n-1} \equiv 1 \pmod{n}$;

9. Докажете, че:
   (i) всяко число на Кармайкъл е свободно от квадрати;
   (ii) всяко число на Кармайкъл е произведение на поне три прости числа;
   (iii) съставното число m е число на Кармайкъл тогава и само тогава, когато за всеки делител p на m е изпълнено, че $p - 1$ дели $m - 1$;
   (iv) най-малкото число на Кармайкъл е 561.

10. Дадена е криптосистема RSA с модул $n = pq$ и шифроваща 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

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

11. 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.

12. 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?

13. 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.

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

15. 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		

16. Дадена е (k, n)-прагова схема над $\mathbb{Z}_{37}$, при която $k = 4$, $n = 6$. Известно е, че дяловете на потребителите A, B, C, D са съответно $(1, 2)$, $(3, 4)$, $(5, 6)$, $(7, 8)$. Да се намери тайният ключ, разпределен между A, B, C и D.

17. 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.)

18. 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 $n = 15049$, $\varphi(n) = 14800$.

19. 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.

20. **Криптосистема на Окамото-Учияма.**

Генериране на ключове. Избираме две големи прости числа p и q, надхвърлящи 2^k за някакво фиксирано k, и пресмятаме $n = p^2q$. 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.

21. 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 $\gcd(e_1, e_2) = 1$.

22. **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 откритият 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).

23. **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. Разглежадме 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.

София, 06.05.2014 г.