2. Въпрос

Определение за синдром на полином за даден цикличен код (едното от двете възможни определения по избор)

Определение за синдром на полином за даден цикличен код

Когато предаваме кодовия полином $c(x)$

по канала, може да има грешки, тогава

$$v(x) = c(x) + e(x),$$

където $e(x)$ е полином на грешка,

тогава $r\big(v(x), g(x)\big)$

се нарича синдром на този полином $S\big(v(x)\big)$,

$$r\big(v(x), g(x)\big) = r\big(c(x) + e(x), g(x)\big) = r\big(e(x), g(x)\big),$$

тогава и само тогава, когато $S\big(v(x)\big) = S\big(e(x)\big)$,

където $r\big(f(x), g(x)\big)$ е остатъкът при делението на $f(x)$ с $g(x)$

3. Въпрос

Опишете двата начина, по които се кодира с цикличен код

Прост начин за кодиране с циклични кодове

$$i(x) \to i(x)g(x) = c(x) \in \mathrm{C}, \deg(i) < k, \deg(g) = n - k,$$

тогава $\deg(c) < n$, този метод е прост,

но от $c(x)$ не може веднага

да се познае $i(x)$,

където $i(x)$ е полином,

който се съпоставяна блок с дължина k.

Систематичен начин за кодиране с циклични кодове

За да съвпадат старшите коефициенти в кодовата дума $c(x)$

с коефициентите на $i(x)$,

тогава $i(x) \to c(x) = x^{n-k}i(x) + t(x)$,

$0 \leq \deg(t) \leq n - k + 1$,

където $t(x)$ е дефиниран като,

$$r\left(x^{n-k}i(x) + t(x), g(x)\right) = 0,$$

тогава и само тогава,

когато $r\left(x^{n-k}i(x) + t(x), g(x)\right) = -t(x)$,

където $r\big(f(x), g(x)\big)$ е остатъкът при делението на $f(x)$ с $g(x)$,

тогава $i(x) = \sum_{j=0}^{k-1} i_j x^j \to c(x) = \sum_{j=0}^{n-1} c_j x^j$, където

коефициентите $c_{n-1}, c_{n-2}, \dots, c_{n-k}$ съвпадат с коефициентите на $i(x)$.

5. Въпрос

Опишете декодиращия алгоритъм на Мегит (за циклични кодове с използване на синдроми)

Стъпки на алгоритъма:

1. Създаване на таблица на синдромите:

Предварително се изчисляват и записват синдромите за всички възможни полиноми грешки с тегло до t (максималният брой грешки, които кодът може да коригира).

Тези синдроми се организират в таблица, която включва всички полиноми грешки и съответните им синдроми

2. Изчисляване на синдрома на получения полином:

При приемане на кодираното съобщение (възможно съдържащо грешки), се изчислява синдромът на получения полином $v(x)$. Това се прави чрез деление на $v(x)$с пораждащия полином $g(x)$, и вземане на остатъка: $S(v(x)) = r(v(x), g(x))$

3. Сравнение със синдромите в таблицата:

Синдромът на получения полином се сравнява с предварително изчислените синдроми в таблицата. Ако намереният синдром съвпада с някой от записаните синдроми, съответният полином грешка се извлича от таблицата.

4. Корекция на грешките:

Ако синдромът съвпадне с някой в таблицата, кодираното съобщение се коригира чрез изваждане на намерения полином грешка от получения полином:
$c(x) = v(x) - d(x)$където $d(x)$ е намереният полином грешка.

5. Последователно проверяване на полиноми:

Ако синдромът на получения полином не е в таблицата, последователно се проверяват синдромите на полиномите $xv(x)$, $x^2v(x)$, … , докато не се намери съвпадение в таблицата.

Когато се намери съвпадение, съответният полином грешка $d(x)$се използва за корекция на получения полином $v(x)$: $c(x) = v(x) - x\hat{}i\ d(x)$
където $x\hat{}i\ v(x)$ е полученият полином, чиито синдром съвпада с някой от таблицата.

6. Точност на декодирането:

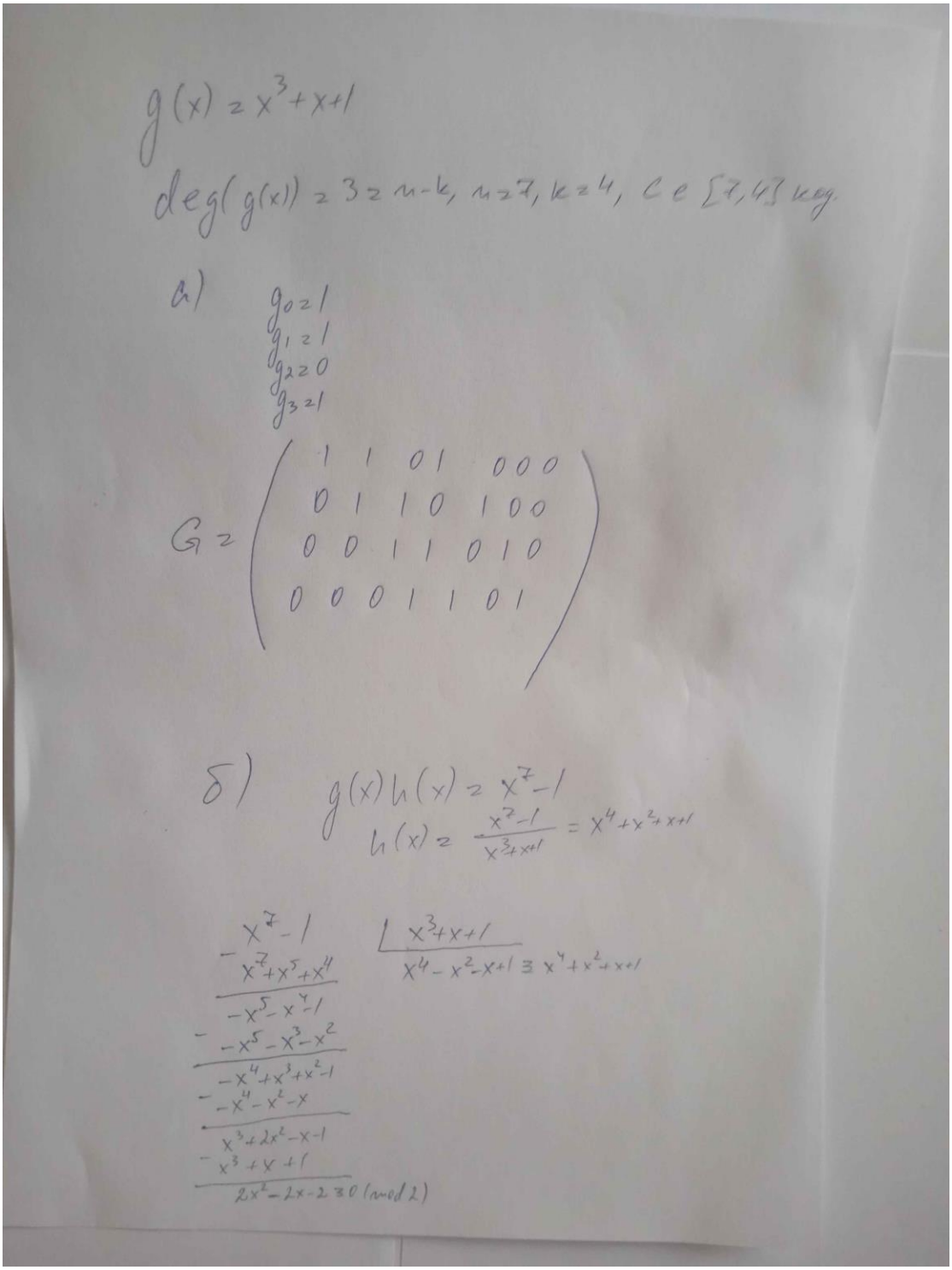
Алгоритъмът гарантира точно декодиране, ако броят на грешките не надвишава капацитета за корекция на грешки t на кода.

6. Въпрос

Нека $C = \langle g(x) \rangle$ е двоичен цикличен код с дължина 7, където $g(x) = x^3 + x + 1$. Да се намери:

а) пораждаща матрица на C;

б) проверовъчна матрица на C.



$h(x) = 1 + x + x^2 + x^4$

$h_0 = 1$
$h_1 = 1$
$h_2 = 1$
$h_3 = 0$
$h_4 = 1$

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

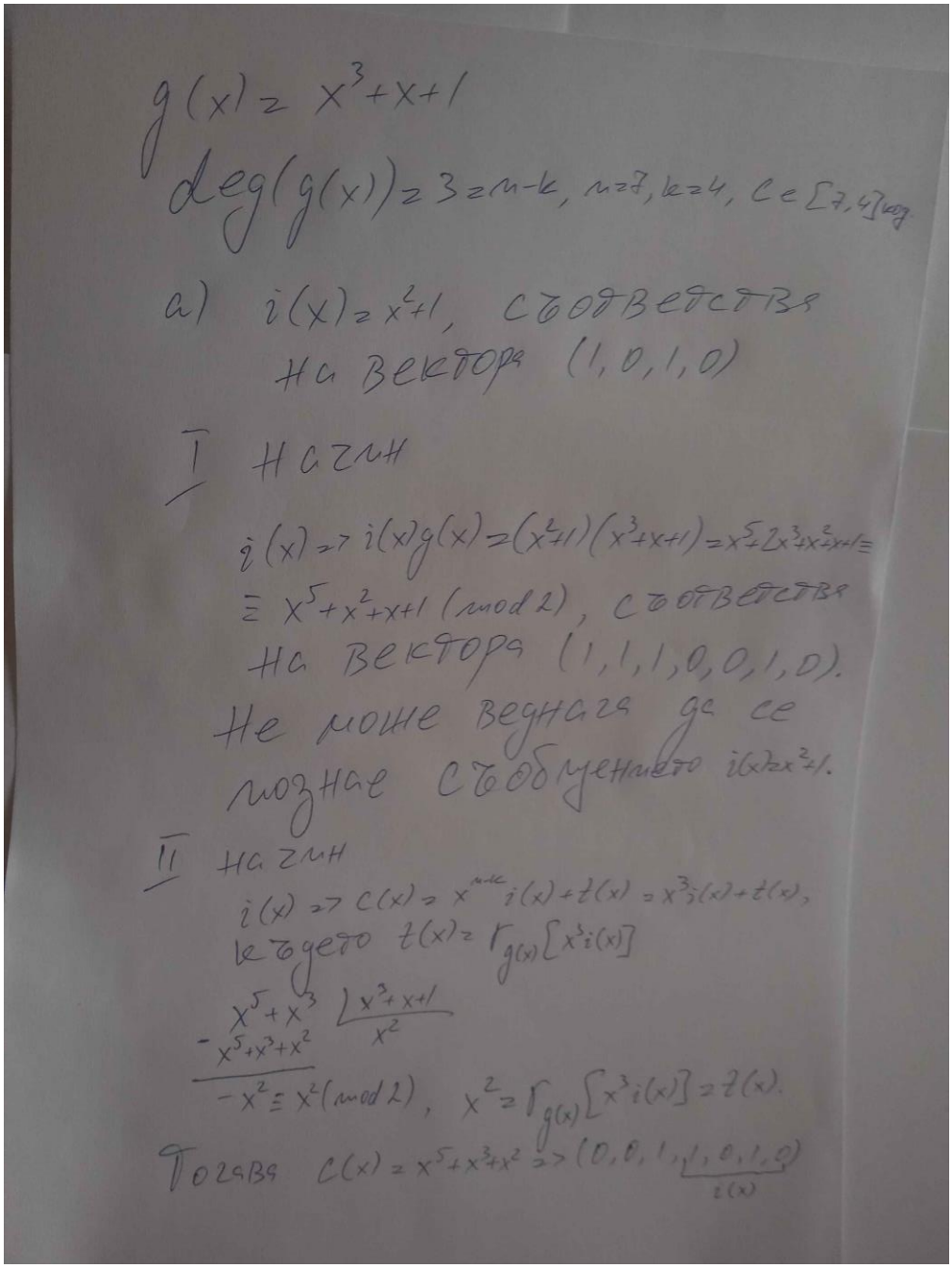
7. Въпрос

Нека $C = \langle g(x) \rangle$ е двоичен цикличен код с дължина 7, където $g(x) = x^3 + x + 1$.

а) кодирайте по двата начина съобщението $x^2 + 1$;

б) ако кодираното съобщение е (1011100), възстановете оригиналното съобщение, получено по двата начина на кодиране;

в) напишете пораждащата и проверовъчната матрица на кода C.



б)

$(1011100) \Rightarrow c(x) = 1 + x^2 + x^3 + x^4$.

Ако е кодирано по I начин, то оригиналното съобщение е

$i(x) = \frac{c(x)}{g(x)} = x+1 \Rightarrow (1,1,0,0)$

$$\begin{array}{r|l} x^4+x^3+x^2+1 & x^3+x+1 \\ \hline x^4+x^2+x & x+1 \\ \hline x^3+x+1 & \\ x^3+x+1 & \\ \hline -2x \equiv 0 \pmod 2 & \end{array}$$

Ако е кодирано по II начин, то последните 4 координати са оригиналното съобщение, (1100).

б) $g(x) = x^3+x+1$, $(1,1,0,1,0,0,0)$

$xg(x) = x^4+x^2+x$, $(0,1,1,0,1,0,0)$

$x^2g(x) = x^5+x^3+x^2$, $(0,0,1,1,0,1,0)$

$x^3g(x) = x^6+x^4+x^3$, $(0,0,0,1,1,0,1)$

Порождающая матрица

$$G = \begin{pmatrix} 1&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&0&1 \end{pmatrix}$$

$g(x)h(x) = x^7-1$

$h(x) = \dfrac{x^7-1}{x^3+x+1} = x^4+x^2+x+1 \pmod 2$

$$\begin{array}{r|l} x^7-1 & x^3+x+1 \\ \hline -x^7+x^5+x^4 & x^4+x^2+x+1 \pmod 2 \\ \hline -x^5-x^4 & \\ -x^5-x^3-x^2 & \\ \hline -x^4+x^3+x^2-1 & \\ -x^4-x^2-x & \\ \hline x^3+2x^2+x-1 & \\ -x^3+x+1 & \\ \hline 2x^2-2 \equiv 0 \pmod 2 & \end{array}$$

Проверочният полином е

$h(x) = 1 + x + x^2 + x^4$

$h_4 = 1$

$h_3 = 0$

$h_2 = 1$

$h_1 = 1$

$h_0 = 1$

Проверочната матрица е

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

8. Въпрос

Определение за криптографска система на Цезар

Криптографската система на Цезар, наричана също шифър на Цезар или Цезарово изместване, е един от най-простите и известни класически шифри. Тя е наречена на Юлий Цезар, който я използвал за шифриране на своите военни съобщения. Шифърът на Цезар е вид шифър с пряка субституция (субституционен шифър) – това означава, че всяка буква се замества само с една и съща друга буква в целия текст.

Описание на алгоритъма:

1. **Избор на ключ**: Изберете цяло число kkk между 1 и 25. Това число ще бъде вашият ключ за шифриране.
2. **Шифриране**:
   - За всяка буква в оригиналния текст (ясен текст):
     - Ако буквата е в азбуката, изместете я с kkk позиции надясно.
     - Ако след изместването буквата премине края на азбуката, започнете отначало от първата буква на азбуката.
   - Буквите, които не са в азбуката (напр. цифри, пунктуационни знаци и т.н.), остават непроменени.
3. **Дешифриране**:
   - За да дешифрирате шифрован текст, изместете всяка буква с kkk позиции наляво.

9. Въпрос.

Определение за криптографска система.

Криптографска система е семейство T от криптографски трансформации за изходен текст. Всяка трансформация от T е с индекс (етикет) k, наречен ключ –T_k. Обикновено ключът също е дума над избраната азбука и се пази в тайна.

- K – множеството на всички възможни стойности за ключовете.
- Криптографската система $T = \{T_k, k \in K\}$, където K е достатъчно голямо множество, обикновено се предполага за известна на опонента (неприятеля).

Съществуват различни системи за генериране и разпределяне на ключовете.

10. Въпрос

Определение за асиметрична криптосистема

Асиметрични криптосистеми (Криптографски системи с публичен ключ) – криптографска система, при която ключа за шифриране E е публично известен, но от него е много трудно да се намери ключа за дешифриране D.

Примери: RSA, Elliptic curve cryptography (ECC), криптографска система на Rabin, ElGamal, McEliece и др.

11. Въпрос

Определение за криптоанализ

Криптоанализът е наука и изкуство, занимаваща се с анализа и разбиването на криптографски системи и шифри. Основната цел на криптоанализа е да открие слабости в криптографските алгоритми, които позволяват извличането на оригиналния текст (ясен текст) от шифрован текст без да се знае ключът, използван за шифриране. Криптоанализът включва различни техники и методи за атакуване на криптографски системи, като създава методи за разбиване (декодиране) на секретни системи като например:

1. **Атаки със изчерпателно претърсване**: Изпробване на всички възможни ключове, докато не се намери правилният.
2. **Статистически атаки**: Използване на статистически свойства на изходния текст или шифротекста за разкриване на информация.
3. **Лингвистични атаки**: Използване на особеностите и честотата на буквите в даден език за разбиване на шифъра.
4. **Атаки с известен текст**: Когато атакуващият има достъп както до ясен текст, така и до съответстващия му шифрован текст.
5. **Атаки с избран текст**: Когато атакуващият може да избира текстовете, които да бъдат шифровани, и да получава съответстващите им шифротексти.
6. **Атаки с избран шифротекст**: Когато атакуващият може да избира шифротексти и да получава съответстващите им ясни текстове.

Криптоанализът играе ключова роля в оценката на сигурността на криптографските системи и е важен инструмент за подобряване и усъвършенстване на криптографските методи.

12. Въпрос

Определение за криптология

Криптологията е математическо направление, което се занимава с проектирането и разбиването на секретни системи. Състои се от два основни дяла:

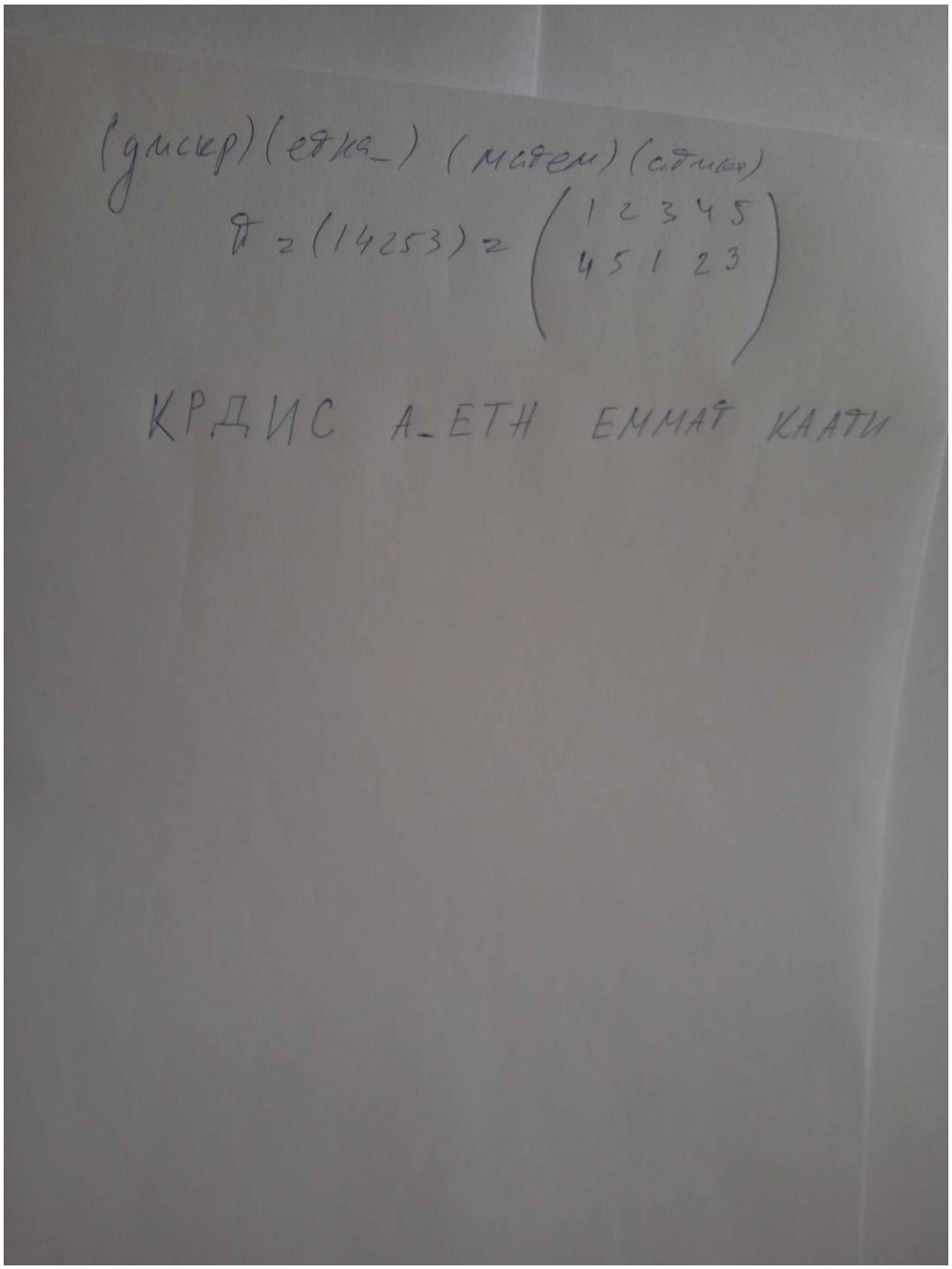
- **Криптография** – създава методи за защита на информационните данни в компютърните системи, банковото дело, медицината, политиката и други области.
- **Криптоанализ** – разработва методи за разбиване (декодиране) на секретни системи.

Криптологията обединява усилията и знанията от тези два дяла, за да осигури сигурност и надеждност на комуникациите и съхранението на данни.

13. Въпрос

Шифрирайте текста: (дискр)(етна_) (матем) (атика) като за ключ използвате пермутацията $\pi = (14253)$.

Линк към решенията:



14. Въпрос

Да се шифрира текста „дойдох,видях,победих" чрез криптографската субституция на Цезар C_4.

Линк към решенията: