Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Разделы спецкурса

- Криптография
- Информационная безопасность
- Анализ данных

Криптография

- Шифры замены, гаммирование
- Симметричное шифрование
- Шифрование с открытым ключом
- Хеш функции
- Криптографические протоколы
- Технология блокчейн, криптовалюты

Компьютерная безопасность

- Форматы и запуск исполняемых файлов
- Исследование и изменение программ
- Средства защиты программ
- Вредоносные программы
- VPN
- Атака по сторонним каналам
- Стеганография

Анализ данных

- Регрессии
- Кластеризация
- Классификация
- Нейронные сети
- Обучение с подкреплением

Гаммирование

Сложение по модулю

Алфавит: $A = \{0, 1, \ldots, N-1\}$

Открытый текст: $p_1\ p_2\ p_3\ p_4\ \ldots \quad p_i \in A$

Гамма: $g_1\ g_2\ g_3\ g_4\ \ldots \quad g_i \in A$

Шифртекст: $c_1\ c_2\ c_3\ c_4\ \ldots \quad c_i \in A$

$$c_i = (p_i + g_i) \bmod N$$

$$p_i = (c_i + N - g_i) \bmod N$$

Побитовое сложение

- Открытый текст: $p_1\ p_2\ p_3\ p_4\ \ldots$
- Гамма: $g_1\ g_2\ g_3\ g_4\ \ldots$
- Шифртекст: $c_1\ c_2\ c_3\ c_4\ \ldots$

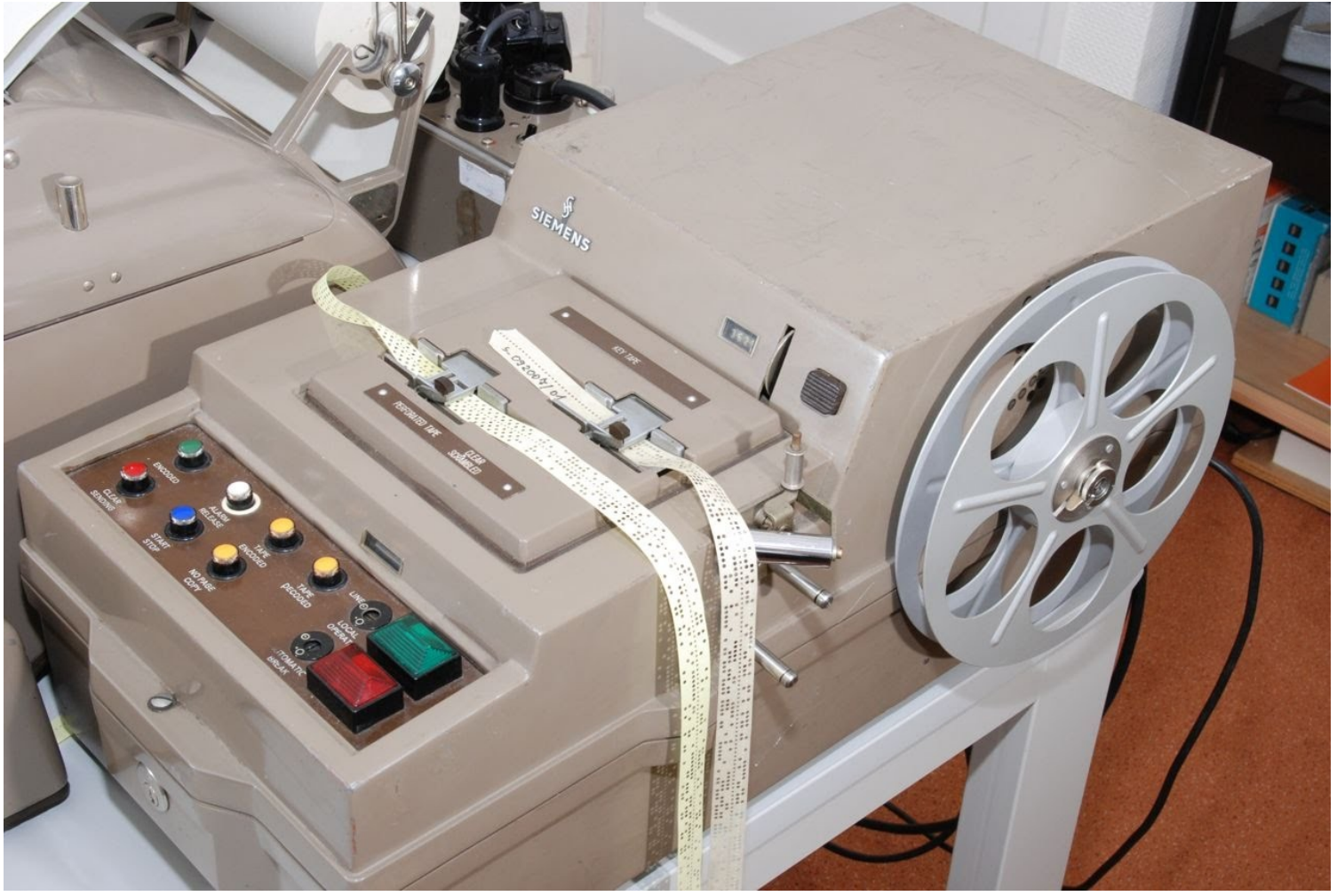
$$c_i = p_i \oplus g_i$$

$$p_i = c_i \oplus g_i$$

Примеры использования

- Если гамма состоит из одного повторяющегося символа, то получается шифр простой замены (шифр Цезаря).
- 1918 году создана пара телеграфных аппаратов, накладывавших гамму на передаваемые сообщения. Гамма находилась на склеенной в кольцо перфоленте.
- Использование одноразовых блокнотов разведчиками во время первой и второй мировых войн.

Шифрующий телеграф



Одноразовый блокнот

Генерация гаммы

- Использование физических процессов (белый шум, космическое излучение, радиационный фон)
- Десятичная запись иррационального числа
- Алгоритмы генерации псевдослучайных чисел ($X_{i+1} = (a*X_i + b) \bmod m$)

Надежность алгоритма

Шифрование наложением гаммы абсолютно надежно, если гамма:

- совершенно случайна
- по длине не меньше текста
- используется один раз

Повторение гаммы

Причины:

- Несколько сообщений зашифрованы на одной гамме
- Гамма короче сообщения

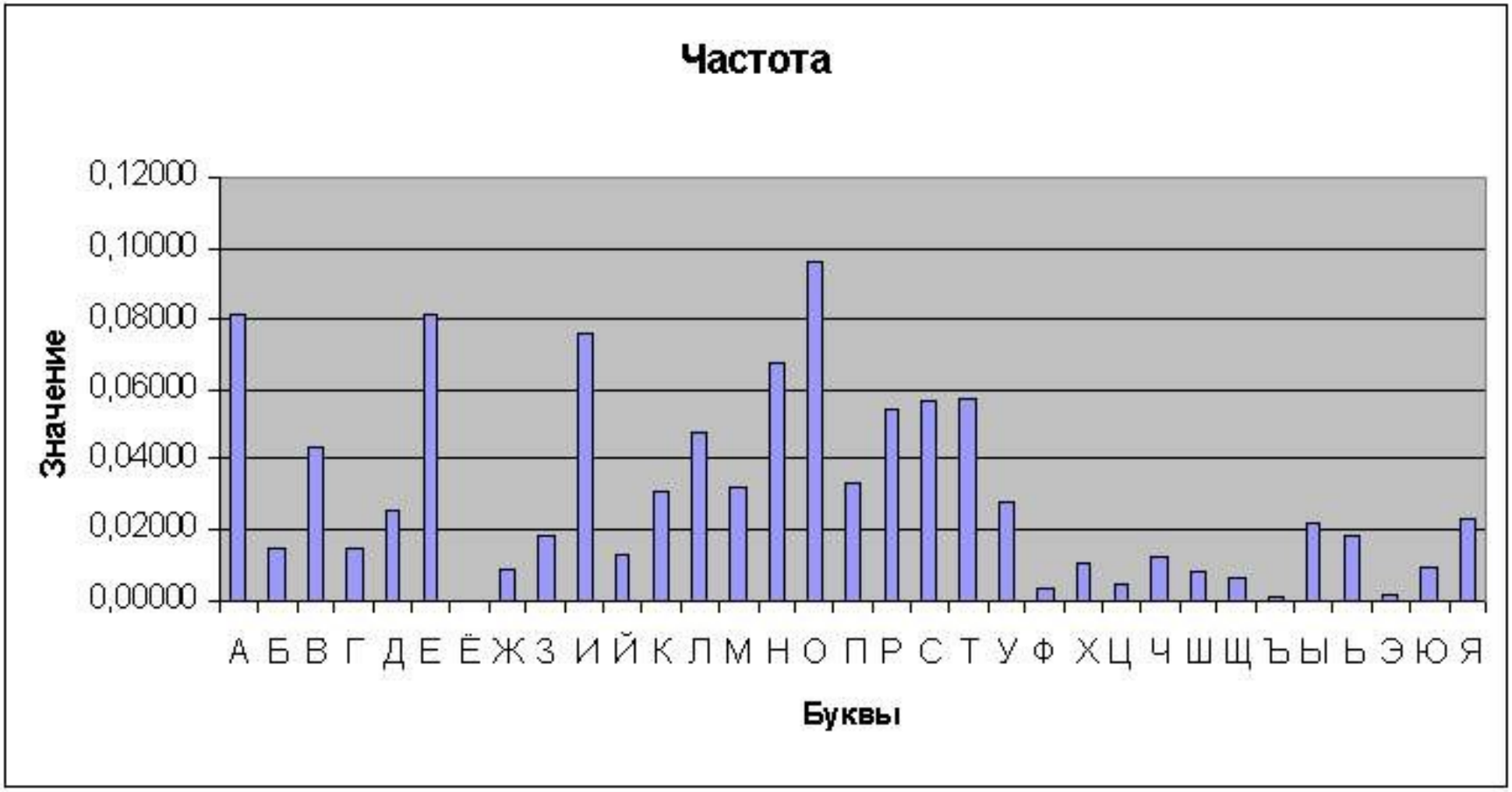
Несколько сообщений на одной гамме

C_1: c_{11} c_{12} c_{13} c_{14} c_{15} …

C_2: c_{21} c_{22} c_{23} c_{24} c_{25} …

C_3: c_{31} c_{32} c_{33} c_{34} c_{35} …

G: * * * * * ...


Частота
0,12000
0,10000
0,08000
0,06000
0,04000
0,02000
0,00000
Значение
А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Буквы

Частота биграмм

1\2	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
а	0,00	0,16	0,45	0,10	0,27	0,23		0,16	0,43	0,04	0,09	0,60	0,97	0,45	0,77	0,01	0,13	0,41	0,53	0,69	0,03	0,03	0,14	0,10	0,15	0,12	0,04				0,00	0,15	0,26
б	0,12	0,00	0,01	0,00	0,00	0,24		0,00	0,00	0,12		0,01	0,13	0,01	0,05	0,37		0,16	0,03	0,00	0,14		0,01	0,00	0,00	0,00	0,05	0,03	0,35	0,00	0,00	0,01	0,05
в	0,84	0,00	0,01	0,01	0,03	0,66			0,04	0,41		0,05	0,17	0,02	0,20	0,89	0,03	0,11	0,32	0,05	0,10		0,01	0,00	0,01	0,07	0,00		0,36	0,02			0,05
г	0,18	0,00	0,00	0,00	0,12	0,08				0,15		0,01	0,14	0,00	0,03	0,98	0,00	0,16	0,00	0,00	0,08				0,00								
д	0,62	0,00	0,10	0,01	0,01	0,68	0,00	0,02	0,00	0,36		0,04	0,11	0,02	0,25	0,52	0,03	0,15	0,08	0,02	0,22		0,01	0,02	0,01	0,01		0,00	0,09	0,05	0,00	0,00	0,04
е	0,03	0,14	0,25	0,34	0,47	0,17	0,00	0,11	0,18	0,02	0,32	0,24	0,75	0,57	1,27	0,05	0,12	0,88	0,70	0,81	0,01	0,02	0,09	0,05	0,15	0,10	0,08				0,00	0,02	0,03
ё													0,00	0,00	0,00			0,00		0,00													
ж	0,13	0,01		0,00	0,12	0,44		0,00		0,19		0,02	0,00	0,00	0,15	0,01		0,00	0,00		0,03				0,01					0,00			
з	0,64	0,02	0,13	0,03	0,12	0,06		0,01	0,00	0,09		0,02	0,03	0,07	0,22	0,11	0,00	0,05	0,00	0,00	0,06			0,00	0,00			0,00	0,07	0,01		0,00	0,03
и	0,07	0,06	0,32	0,09	0,19	0,39		0,04	0,36	0,23	0,24	0,35	0,55	0,42	0,57	0,09	0,04	0,21	0,44	0,64	0,00	0,02	0,28	0,12	0,26	0,07	0,02				0,00	0,08	0,36
й		0,00	0,00	0,00	0,02	0,00			0,00			0,02	0,01	0,01	0,05	0,01		0,00	0,10	0,03		0,00		0,01	0,02	0,01							
к	0,90		0,04	0,00	0,00	0,10		0,01	0,00	0,50		0,00	0,11	0,00	0,04	1,23	0,00	0,22	0,07	0,18	0,24		0,00	0,03		0,00							
л	0,70	0,00	0,00	0,02	0,01	0,70	0,00	0,04	0,00	0,93		0,05	0,05	0,00	0,06	0,69	0,00	0,00	0,12	0,01	0,17		0,00		0,01	0,00			0,07	0,69		0,14	0,26
м	0,42	0,01	0,00	0,00		0,56			0,00	0,46		0,02	0,03	0,03	0,17	0,51	0,05	0,01	0,02	0,00	0,26	0,00	0,00	0,00	0,00				0,18	0,01	0,00	0,00	0,06
н	1,42	0,00	0,01	0,03	0,08	1,15		0,00	0,01	1,25		0,09	0,00		0,46	1,56	0,00	0,01	0,13	0,20	0,28	0,02	0,00	0,07	0,02	0,00	0,01		0,66	0,13	0,00	0,02	0,18
о	0,01	0,54	1,18	0,67	0,74	0,28		0,26	0,20	0,12	0,58	0,29	0,81	0,77	0,71	0,06	0,22	0,83	0,96	0,85	0,01	0,04	0,07	0,04	0,24	0,10	0,03				0,02	0,03	0,09
п	0,23		0,00			0,33				0,15		0,01	0,13		0,02	1,25	0,02	1,02	0,01	0,01	0,10			0,00	0,00	0,00			0,04	0,01			0,03
р	1,22	0,02	0,06	0,06	0,04	0,96		0,05	0,01	0,68		0,05	0,01	0,08	0,14	1,14	0,02	0,02	0,08	0,12	0,38	0,01	0,02	0,01	0,01	0,03	0,00		0,20	0,06	0,00	0,02	0,12
с	0,24	0,01	0,18	0,00	0,03	0,46	0,00	0,00	0,00	0,28		0,62	0,36	0,10	0,15	0,46	0,26	0,06	0,19	1,74	0,15	0,01	0,03	0,01	0,05	0,02		0,00	0,05	0,29	0,00	0,02	0,48
т	0,88	0,01	0,42	0,00	0,02	0,80			0,00	0,66		0,10	0,03	0,01	0,20	1,64	0,01	0,49	0,26	0,01	0,21	0,00	0,00	0,01	0,02	0,00	0,00	0,00	0,20	0,74	0,00	0,01	0,07
у	0,02	0,09	0,06	0,12	0,25	0,05		0,17	0,05	0,00	0,01	0,11	0,15	0,12	0,06	0,00	0,11	0,14	0,19	0,20		0,00	0,05	0,00	0,15	0,07	0,05				0,00	0,17	0,01
ф	0,03			0,00		0,06				0,07			0,01		0,00	0,07		0,02	0,00	0,01	0,01	0,01							0,00	0,00			
х	0,08		0,02	0,00		0,01				0,04			0,01	0,01	0,03	0,27		0,03	0,01	0,00	0,02		0,00			0,00					0,00		
ц	0,07		0,01			0,15				0,24		0,01				0,02			0,00		0,02								0,03				
ч	0,27		0,00			0,55	0,00			0,25		0,05	0,01		0,15	0,01		0,00		0,33	0,06					0,02				0,03			
ш	0,10		0,00			0,25				0,19		0,06	0,06	0,00	0,04	0,03	0,00	0,00		0,02	0,03			0,00						0,06			
щ	0,05					0,22	0,00			0,13					0,01			0,00			0,02									0,01			
ъ						0,03																											0,02
ы		0,03	0,13	0,01	0,02	0,21		0,01	0,01	0,00	0,21	0,03	0,19	0,18	0,03		0,03	0,03	0,09	0,09			0,24	0,00	0,02	0,05	0,00						0,00
ь		0,01	0,00	0,01	0,01	0,05			0,03	0,01		0,12		0,03	0,29	0,00	0,00		0,13	0,03		0,00		0,01	0,01	0,07	0,00					0,06	0,04
э			0,00		0,00				0,00		0,00	0,04	0,02	0,01	0,01		0,01	0,01	0,01	0,29		0,01	0,00										
ю		0,04		0,00	0,05			0,00	0,01			0,01	0,01	0,01	0,01			0,02	0,02	0,12			0,00	0,01	0,02	0,00	0,08					0,00	
я		0,01	0,06	0,01	0,06	0,04		0,02	0,05	0,00	0,01	0,02	0,08	0,06	0,08		0,01	0,02	0,05	0,20			0,04	0,01	0,02	0,00	0,04					0,03	0,01

Определение первого символа гаммы

C_1: $\mathbf{c_{11} \oplus g_1 = t_{11}}$ c_{12} c_{13} c_{14} c_{15} …

C_2: $\mathbf{c_{21} \oplus g_1 = t_{21}}$ c_{22} c_{23} c_{24} c_{25} …

C_3: $\mathbf{c_{31} \oplus g_1 = t_{31}}$ c_{32} c_{33} c_{34} c_{35} …

G: $\mathbf{g_1}$ * * * * …

$P'(G[1] = 0) = v(c_{11} \oplus 0) + v(c_{21} \oplus 0) + v(c_{31} \oplus 0)$

$P'(G[1] = 1) = v(c_{11} \oplus 1) + v(c_{21} \oplus 1) + v(c_{31} \oplus 1)$

…

$P'(G[1] = 32) = v(c_{11} \oplus 32) + v(c_{21} \oplus 32) + v(c_{31} \oplus 32)$

Формула Байеса

$P(A|B) = P(AB) / P(B)$

A – текущий символ в тексте равен y

B – предыдущие k символов равны $x_1, x_2, \ldots, x_k$

$P(AB) = P(x_1 \ldots x_k y)$

$P(y|x_1 \ldots x_k) = P(x_1 \ldots x_k y) / P(x_1 \ldots x_k) = v(x_1 \ldots x_k y) / v(x_1 \ldots x_k)$

Определение второго символа гаммы

C_1: t_{11} $\mathbf{c_{12} \oplus g_2 = t_{12}}$ c_{13} c_{14} c_{15} …

C_2: t_{21} $\mathbf{c_{22} \oplus g_2 = t_{22}}$ c_{23} c_{24} c_{25} …

C_3: t_{31} $\mathbf{c_{32} \oplus g_2 = t_{32}}$ c_{33} c_{34} c_{35} …

G: g_1 $\mathbf{g_2}$ * * * …

$P'(G[2] = g_2|g_1) = P(t_{12}|t_{11}) + P(t_{22}|t_{21}) + P(t_{32}|t_{31}) = v(t_{11}t_{12})/v(t_{12}) + v(t_{21}t_{22})/v(t_{22}) + v(t_{31}t_{32})/v(t_{32})$

Определение третьего символа гаммы

C_1: t_{11} t_{12} $\mathbf{c_{13} \oplus g_3 = t_{13}}$ c_{14} c_{15} …

C_2: t_{21} t_{22} $\mathbf{c_{23} \oplus g_3 = t_{23}}$ c_{24} c_{25} …

C_3: t_{31} t_{32} $\mathbf{c_{33} \oplus g_3 = t_{33}}$ c_{34} c_{35} …

G: g_1 g_2 $\mathbf{g_3}$ * * …

$P'(G[3] = g_3|g_1g_2) = P(t_{13}|t_{11}t_{12}) + P(t_{23}|t_{21}t_{22}) + P(t_{33}|t_{31}t_{32}) =$

$v(t_{11}t_{12}t_{13})/v(t_{11}t_{12}) + v(t_{21}t_{22}t_{23})/v(t_{21}t_{22}) + v(t_{31}t_{32}t_{33})/v(t_{31}t_{32})$

Определение четвертого символа гаммы

C_1: t_{11} t_{12} t_{13} $\mathbf{c_{14} \oplus g_4 = t_{14}}$ c_{15} …

C_2: t_{21} t_{22} t_{23} $\mathbf{c_{24} \oplus g_4 = t_{24}}$ c_{25} …

C_3: t_{31} t_{32} t_{33} $\mathbf{c_{34} \oplus g_4 = t_{34}}$ c_{35} …

G: g_1 g_2 g_3 $\mathbf{g_4}$ * …

$$P'(G[4] = g_4|g_2g_3) = P(t_{14}|t_{12}t_{13}) + P(t_{24}|t_{22}t_{23}) + P(t_{34}|t_{32}t_{33}) =$$

$$v(t_{12}t_{13}t_{14})/v(t_{12}t_{13}) + v(t_{22}t_{23}t_{24})/v(t_{22}t_{23}) + v(t_{32}t_{33}t_{34})/v(t_{32}t_{33})$$

Определение последующих символов гаммы

$$P'(G[n] = g_n | g_{n-2} g_{n-1}) = v(t_{1n-2} t_{1n-1} t_{1n}) / v(t_{1n-2} t_{1n-1}) + v(t_{2n-2} t_{2n-1} t_{2n}) / v(t_{2n-2} t_{2n-1}) + v(t_{3n-2} t_{3n-1} t_{3n}) / v(t_{3n-2} t_{3n-1})$$

При расшифровывании “протягивают” не одну, а несколько наиболее вероятных гамм.

Текст, зашифрованный на короткой гамме

ыофтшлзылтшвшутштвжшнъшлъулткккюфищфаторцлесоокыяхьжцшбдуфъмащясйпншьечшсцузхпенюифйнщаичпрзужцмдыб
жяьоэьтцьяшбоцфлйтвфбтщасщшврюыихоькехпмхонйенщрснтвчуфъпсэупцгуэцоиыьхонийтщфгооацмзнуошагтэсэооцьцрщсл
шмрявюкээьмщшсыузцьовурхшйэьфттсньистмыоъхшгщрсплустихтявасэшткьзхэмуыцъэхщаиушсзупымзпьшхэтзрзшэгщъпръе
аьхдлыншгтшммйхцчимйоцтнряпцьркыгкыюоювпжомяхичоншлцчсютскшлзяхктечьфъквлщфзьеъуудмрлятрмовыссяотнлхсану
знчикпюумдыбжцукщъриьешьъиытщршцоицржуквшббщщуьшгзыьныинштхбзиьоъьфъэпрыяткмъюляпмъюиооеняилшвжшгпев
лщлщжеоььнноцкфттеьъгпчырягчшгуядцхьгцпрфрляргцищаецъоэопршнмйокщоптикфеурфъъагыспкслщихчочеишчочохуксшь
потлраийпзооощьухогкылудснномйоцфахпцмьоьъгпкнщъгщхочасячосуонснжчкицоххгпксэьмтшйшошцоицявфклзелафацухяпт
жюриоцлалрлыцтуынофъгужчужницоцьйнфоэьугупщтгкклряорбтщятшкшургутсэьвуткыьынчырьжыъцжеишчыряцэкруцунсашы
гзфуььъткмуююйквьлхцшчрыямэршьтиялщпюушдюжрцьахехцлыцьзирешуфъпръцпцыипухдтвьтсъшгщпюушпыьтрьашьерчнж
ъкищааьпяьохойньскьхцонщссеьооьецсдюггфшжшьдгхонэвъжмуыцъыдрщгъжскэязчычпюккюэцргпвьаунбиььенъшрырцоасуф
хпзшонццычцрицлйтяфткщасшемуъюхкчуыгнцишаишпсщргъжскятнъвщссксгцнзифахаскорюсехпзлэрцщррфзнбечяниречяоцм
оэонцптщерцмпрегъхешцичъоухенхнлюгщфоцкррфонохцьгщяхдфоэьугусутиущощтгужиъьшцоицыгцьсэоехшгщелхшвшцницо
цьзцучрщскпкшуфтшлзшсшкзъюлчшмуыгущоэьпеьоъуукшенэияктцуррпипойнщруэлщевлщилшпыузяэвьаериошпищщррююкч
онхжуйджргучавцрцмнушгтшнрерцтпщасфэедуъъшиьопъштюэсшчоьъсъъецыгхпгщцеронщпюушчэьхццущеихжхщаиушсзыгяк
тзюгпноньухкоьагужнжгйнлынжлэмрлятрмовыссчеуянуичлнлэшзкцрибишьехткьъсъъецшгтьоъюлкечшьлмкжрясщфухьмиммря
хнытрълщштэуртшмшунцьоыьжцмыььнццеыыслшпыурнлррфихтяхонйенлщбмпйшцкапгщэсушжрылзтрлхерьикянцьоыйпрчев
ужцпмюсскшруаяеьомйояплщритхеэбйнсаънхдоеьнхщъепыилшрщяхитпцьххшгщяоцрешцвщщрщяимжюуядцхьгьбуесуыссыо
эунатмщатцытщнрхшгщэязчсэргоплэйпмкжрхиупнщргъемццщциьэурщуажлфтвршгфтитхгтштщююэыикщлтъогуъхеехонбплщ
енрчощтцапвцурхеехюгщчонохгпгцокттнщехцьомйоцмнръсяпнзяхшкншьикшвтсозоерссщмеэцоиыьхонйэдэьзиреньфъшрсурх
шсэктцрацбмйелуяпгылубпхшвэьйнмрръвфплзшгушклшдыотщцднсучцицоеэьрйелняхиъыфяскпргурхшомьуккншймяпршймьъ
ахясщеплрырциьнтынонцщицищтриьоцкнцпщртишрацофддфоршгттнлыиньощылпксэужрмацявктдуъсопллнрнэдлщвъжскэурхи
вцмрспщтричкщрслшжущиъктщюъихачоррвклрфзыкщъничнлнкищавшгхчакцкихиэовутцщпюушвжпурьоъьърчоныляжишьзимн
щбйньахехцэжрсцщьошоъиханйфъэплаящтзлньньишозитвюгеиьклгилшдрчфъмиэуодчомйоцбтщасщшлутрцбишьехтчзурцшн
мйоклеьэстшйьаенпрщжлумоцьфгтпщттръаццрцндлрхцыкрьднтмуюцткмуссушвюэсушжлэуцорлыргплщшхрчатоорьыфцорщку
чфъшл

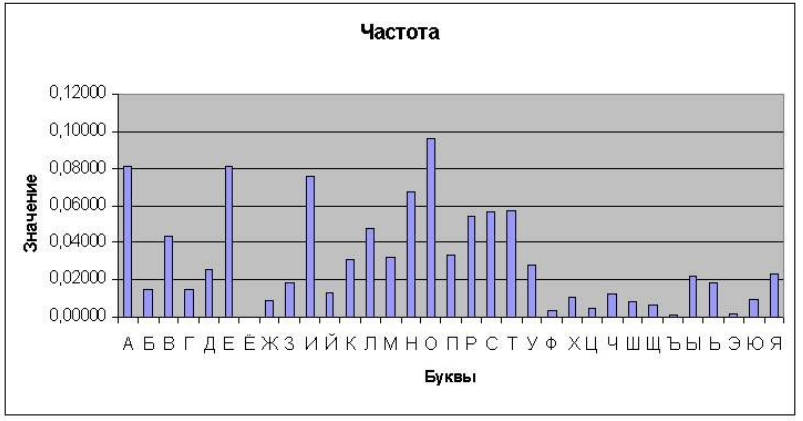
Короткая гамма

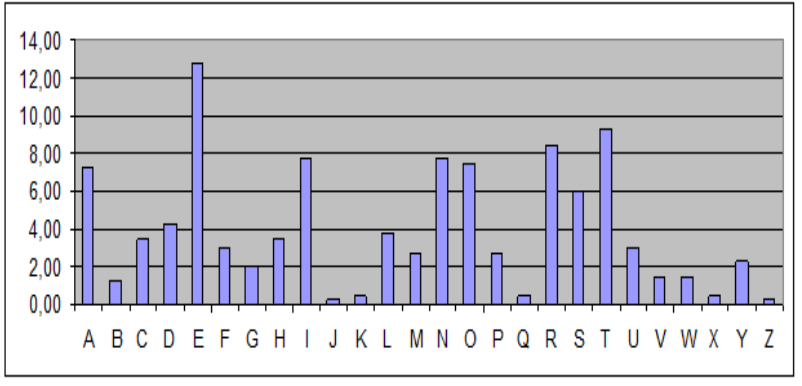
$G = g_1\ g_2\ g_3\ g_4\ g_5$

g_1	$c_1\ c_6\ c_{11}\ c_{16}\ \ldots\ C_1$
g_2	$c_2\ c_7\ c_{12}\ c_{17}\ \ldots\ C_2$
g_3	$c_3\ c_8\ c_{13}\ c_{18}\ \ldots\ C_3$
g_4	$c_4\ c_9\ c_{14}\ c_{19}\ \ldots\ C_4$
g_5	$c_5\ c_{10}\ c_{15}\ c_{20}\ \ldots\ C_5$

- C_1, C_2, C_3, C_4, C_5 – шифры Цезаря

Индекс совпадений





$$I(\vec{x}) = \sum_{i=1}^{m} p_i^2$$

Литературный текст

- русский 0.0553
- английский 0.0644

Случайный текст

- русский 0.0303
- английский 0.0385

Индекс Фридмана

$$I(\vec{x}) = \sum_{i=1}^{m} \frac{f_i (f_i - 1)}{n (n - 1)}$$ - индекс Фридмана

- m – размер алфавита
- n – длина текста
- f_i – количество символов i в тексте

“клара у карла украла кораллы, а карл у клары украл кларнет”

к – 8, л – 9, а – 12, р – 8, у – 4, о – 1, ы – 2, н – 1, е – 1, т – 1

I = (8*7 + 9*8 + 12*11 + 8*7 + 4*3 + 1*0 + 2*1 + 1*0 + 1*0 + 1*0) / (47*46) = 0.152636

Индекс Фридмана

$G = g_1\ g_2\ g_3\ g_4\ g_5$

g_1	$c_1\ c_6\ c_{11}\ c_{16}\ \dots\ C_1$
g_2	$c_2\ c_7\ c_{12}\ c_{17}\ \dots\ C_2$
g_3	$c_3\ c_8\ c_{13}\ c_{18}\ \dots\ C_3$
g_4	$c_4\ c_9\ c_{14}\ c_{19}\ \dots\ C_4$
g_5	$c_5\ c_{10}\ c_{15}\ c_{20}\ \dots\ C_5$

Вычислить индексы Фридмана для C_1, C_2, C_3, C_4, C_5 и усреднить (для нашего текста получится 0.034672).

Индекс Фридмана нашего текста для различных длин гамм

L	I(x)	L	I(x)
1	0.034835	11	0.034404
2	0.041062	12	0.056859
3	0.043894	13	0.034773
4	0.041000	14	0.041195
5	0.034672	15	0.044570
6	0.057197	16	0.040650
7	0.034829	17	0.034906
8	0.040718	18	0.057905
9	0.044010	19	0.034662
10	0.041248	20	0.040894

Литературный – 0.0553

Случайный – 0.0303

Длина гаммы равна 6.

Взаимный индекс совпадений

$$MI(\vec{x}, \vec{y}) = \sum_{i=1}^{m} \frac{f_i g_i}{n_1 n_2}$$

- m – размер алфавита
- n_1 – длина текста x
- f_i – количество символов i в тексте x
- n_2 – длина текста y
- g_i – количество символов i в тексте y

Максимального значения взаимный индекс совпадения достигает в том случае, когда тексты x и y зашифрованы с использованием одного и того же шифра простой замены.

Связь между шифрами

$C_1 = ЛТ_1 + g_1$

$C_2 = ЛТ_2 + g_2$

$C_1 + (g_2 – g_1) = ЛТ_1 + g_2$

C_2 и $C_1 + (g_2 – g_1)$ – одинаковые шифры

Взаимный индекс совпадения строк нашего текста

Sh	MI(c_0,c_1)	Sh	MI(c_0,c_1)	Sh	MI(c_0,c_1)
0	0.026505	11	0.036278	22	0.030522
1	0.020501	12	0.056945	23	0.026351
2	0.025044	13	0.039406	24	0.023082
3	0.035495	14	0.031259	25	0.031453
4	0.025868	15	0.035607	26	0.034505
5	0.023795	16	0.033168	27	0.025698
6	0.033138	17	0.033439	28	0.023612
7	0.034464	18	0.031813	29	0.024625
8	0.037562	19	0.022652	30	0.030793
9	0.043695	20	0.026705	31	0.029621
10	0.033014	21	0.033386		

Взаимный индекс совпадения первой и второй строки при различных сдвигах алфавита второй строки.

Взаимный индекс совпадения строк нашего текста

Sh	$MI(c_0,c_1)$	Sh	$MI(c_0,c_1)$	Sh	$MI(c_0,c_1)$
0	0.024826	11	0.030788	22	0.034193
1	0.031041	12	0.027153	23	0.038564
2	0.036143	13	0.023565	24	0.033639
3	0.025715	14	0.029786	25	0.037945
4	0.023206	15	0.034705	26	0.033969
5	0.023129	16	0.036125	27	0.024991
6	0.030387	17	0.038982	28	0.030334
7	0.029362	18	0.031919	29	0.033297
8	0.022899	19	0.034953	30	0.030440
9	0.021951	20	0.054547	31	0.027017
10	0.024914	21	0.039518		

Взаимный индекс совпадения первой и третьей строки при различных сдвигах алфавита третьей строки.

Гамма

Значения сдвигов букв гаммы относительно первой:

0, 12, 20, 4, 31, 12

Исходная гамма: “машина”

м = (а + 12) % 32

м = (ш + 20) % 32

м = (и + 4) % 32

м = (н + 31) % 32

Оригинальный текст

раскольниковнепривыкктолпеикакужесказанобежалвсякогообществаособенновпоследнееевремянотеперьеговдругчтотопотянулоклюдямчтотосовершалосьвнемкакбыновоеивместестемощутиласькакаятожаждалюдейонтакусталотцелогомесяцаэтойсосредоточеннойтоскисвоейимрачноговозбужденияччтохотяоднуминутухотелосьемувздохнутьвдругоммирехотьбывкакомбытонибылоинесмотрянавсюгрязьобстановкионсудовольствиемоставалсятеперьвраспивочнойхозяинзаведениябылвдругойкомнатеночастовходилвглавнуюспускаясьвнееоткудатопоступенькампричемпреждевсеговыказывалисьегощегольскиесмазныесапогисбольшимикраснымиотворотамионбылвподдевкеивстрашнозасаленномчерноматласномжилетебезгалстукаавслицоегобылокакбудтосмазаномасломточножелезныйзамокзазастойкойнаходилсямальчишкалетчетырнадцатиибылдругоймальчишкамоложекоторыйподавалесличтоспрашивалистояликрошеныеогурцычерныесухариирезаннаякусочкамирыбавсэтооченьдурнопахлобылодушнотакчтобылодаженестерпимосидетьивсдотогобылопропитановиннымзапахомчтокажетсяотодногоэтоговоздухаможнобыловпятьминутсделатьсяпьянымбываютиныевстречисовершеннодажеснезнакомыминамлюдьмикоторымимыначинаеминтересоватьсяспервоговзглядакактовдругвнезапнопреждечемскажемсловотакоеточновпечатлениепроизвелнараскольниковатотгостькоторыйсиделпоодальипоходилнаотставногочиновникамолодойчеловекнесколькоразпри поминалпотомэтопервоевпечатлениеидажеприписывалегопредчувствиюонбеспрерывновзглядывалначиновникаконечноипотомуещечтоисамтотупорносмотрелнанегоивиднобылочтотомуоченьхотелосьначатьразговорнаостальныхжебывшихвраспивочнойнеисключаяихозяиначиновниксмотрелкактопривычноидажесоскукойавместестемисоттенкомнекотороговысокомерногопренебрежениякакбыналюдейнизшегоположенияиразвитияскоторыминечегоемуговоритьэтобылчеловеклетужезапятьдесятсреднегоростаиплотногосложенияспроседьюисбольшоюлысинойсотекшимотпостоянногопьянстваженлтымдажезеленоватымлицомисприпухшимивекамииззакоторыхсияликрошечныекакщелочкиноодушевленныекрасноватыеглазкиночтотобыловнемоченьстранноевовзглядеегосветиласькакбудтодажевосторженностьпожалуйбылисмыслиумновтожевремямелькалокакбудтоибезумиеодетонбылвстарыйсовершеннооборванныйчерныйфраксосыпавшимисяпуговицамиоднатолькоещедержаласькоекакинанеетоонизастегивалсявидиможелаянеудалятьсяприличийизподнанковогожилетаторчаламанишкавсяскомканнаязапачканнаяизалитаялицобыловыбритопочиновничьинодавноужетакчтоужегустоначалавыступатьсизаящетинадаивухваткахегодействительнобылочтотосолидночиновничьеноонбылвбеспокойствеерошилволосыиподпиралиногдавтоскеобеимирукамиголовуположапродранныелоктиназалитыйилипкийстол

```cpp
#include "crypto_tools.h"
#include "io_tools.h"

using namespace std;

vector<uint8_t> find_gamma(
    const vector<uint8_t>& data
    )
{
    uint8_t gamma_length;
    vector<vector<uint8_t>> lines;
    vector<uint8_t> shifts(1, 0);

    gamma_length = CryptoTools::find_gamma_length(data, 20);
    lines = CryptoTools::split_text_into_gamma_lines(data, gamma_length);

    for (uint8_t i = 1; i < gamma_length; i++)
        shifts.push_back(CryptoTools::find_lines_shift(lines[0], lines[i]));

    return shifts;
}


int main()
{
    vector<uint8_t> gamma = {0x0c, 0x00, 0x18, 0x08, 0x0d, 0x00}; // "машина"
    vector<uint8_t> data = IoTools::read_file("/home/user/Work/Solutions/Sssc/ShortGamma/data.txt");

    data = CryptoTools::apply_gamma(data, gamma);
    vector<uint8_t> shifts = find_gamma(data);

    return 0;
}
```