БУ ВО Ханты – Мансийского автономного округа – Югры

«Сургутский государственный университет»

Политехнический институт

Кафедра автоматики и компьютерный систем

**ЛАБОРАТОРНАЯ РАБОТА №5**

по дисциплине: «Основы защиты информации»

по теме: «Потоковое шифрование»

Выполнила: студентка группы №609-11

Пашина Илона Руслановна

Приняла: старший преподаватель кафедры АиКС

Кривицкая Марина Александровна

Сургут

2025 г.

**Тема**: поточное шифрование.

**Задание на лабораторную работу:**

1. реализовать поточное шифрование с собственным генератором псевдослучайных чисел.

**Среда реализации**: любая.

**Методические указания:**

В качестве ГПСЧ допустимо использовать любой алгоритм за исключением конгруэнтных генераторов. (Был использован метод Фибоначчи с запаздываниями)

**Листинг**

package main

import (

"fmt"

)

func CodedByFibonachi(a, b int, message string, k []float32) string {

runes := []rune(message)

size := len(runes)

for i := 0; i < size; i++ {

if i >= len(k) {

k = append(k, helper(a, b, i, k))

}

key := int32(k[i] \* 100)

runes[i] = runes[i] ^ key

}

return string(runes)

}

func helper(a, b, i int, k []float32) float32 {

temp := k[i-a] - k[i-b]

if temp < 0 {

temp += 1.

}

return temp

}

func main() {

a, b := 17, 5

k := []float32{0.324, 0.125, 0.153, 0.545, 0.541, 0.879, 0.147, 0.658, 0.354, 0.912, 0.456, 0.694, 0.954, 0.357, 0.014, 0.751, 0.469}

message := "Hello, World!shfgdcfjahdgbhlskvjhfioshgliwysgbedhjblwjed"

message = "Задача организации, в особенности же внедрение современных методик представляет собой интересный эксперимент проверки первоочередных требований. В рамках спецификации современных стандартов, действия представителей оппозиции представляют собой не что иное, как квинтэссенцию победы маркетинга над разумом и должны быть превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. В рамках спецификации современных стандартов, сторонники тоталитаризма в науке освещают чрезвычайно интересные особенности картины в целом, однако конкретные выводы, разумеется, превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. Учитывая ключевые сценарии поведения, внедрение современных методик представляет собой интересный эксперимент проверки переосмысления внешнеэкономических политик. Задача организации, в особенности же граница обучения кадров в значительной степени обусловливает важность дальнейших направлений развития. Кстати, сделанные на базе интернет-аналитики выводы, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут функционально разнесены на независимые элементы. Современные технологии достигли такого уровня, что постоянный количественный рост и сфера нашей активности однозначно определяет каждого участника как способного принимать собственные решения касаемо направлений прогрессивного развития. Но убеждённость некоторых оппонентов напрямую зависит от позиций, занимаемых участниками в отношении поставленных задач. Картельные сговоры не допускают ситуации, при которой диаграммы связей заблокированы в рамках своих собственных рациональных ограничений. Противоположная точка зрения подразумевает, что явные признаки победы институционализации, превозмогая сложившуюся непростую экономическую ситуацию, заблокированы в рамках своих собственных рациональных ограничений. Как принято считать, элементы политического процесса, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут представлены в исключительно положительном свете. Учитывая ключевые сценарии поведения, консультация с широким активом предопределяет высокую востребованность первоочередных требований. Значимость этих проблем настолько очевидна, что убеждённость некоторых оппонентов влечет за собой процесс внедрения и модернизации дальнейших направлений развития. Для современного мира реализация намеченных плановых заданий представляет собой интересный эксперимент проверки стандартных подходов. В целом, конечно, экономическая повестка сегодняшнего дня однозначно определяет каждого участника как способного принимать собственные решения касаемо кластеризации усилий.Задача организации, в особенности же внедрение современных методик представляет собой интересный эксперимент проверки первоочередных требований. В рамках спецификации современных стандартов, действия представителей оппозиции представляют собой не что иное, как квинтэссенцию победы маркетинга над разумом и должны быть превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. В рамках спецификации современных стандартов, сторонники тоталитаризма в науке освещают чрезвычайно интересные особенности картины в целом, однако конкретные выводы, разумеется, превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. Учитывая ключевые сценарии поведения, внедрение современных методик представляет собой интересный эксперимент проверки переосмысления внешнеэкономических политик. Задача организации, в особенности же граница обучения кадров в значительной степени обусловливает важность дальнейших направлений развития. Кстати, сделанные на базе интернет-аналитики выводы, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут функционально разнесены на независимые элементы. Современные технологии достигли такого уровня, что постоянный количественный рост и сфера нашей активности однозначно определяет каждого участника как способного принимать собственные решения касаемо направлений прогрессивного развития. Но убеждённость некоторых оппонентов напрямую зависит от позиций, занимаемых участниками в отношении поставленных задач. Картельные сговоры не допускают ситуации, при которой диаграммы связей заблокированы в рамках своих собственных рациональных ограничений. Противоположная точка зрения подразумевает, что явные признаки победы институционализации, превозмогая сложившуюся непростую экономическую ситуацию, заблокированы в рамках своих собственных рациональных ограничений. Как принято считать, элементы политического процесса, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут представлены в исключительно положительном свете. Учитывая ключевые сценарии поведения, консультация с широким активом предопределяет высокую востребованность первоочередных требований. Значимость этих проблем настолько очевидна, что убеждённость некоторых оппонентов влечет за собой процесс внедрения и модернизации дальнейших направлений развития. Для современного мира реализация намеченных плановых заданий представляет собой интересный эксперимент проверки стандартных подходов. В целом, конечно, экономическая повестка сегодняшнего дня однозначно определяет каждого участника как способного принимать собственные решения касаемо кластеризации усилий.Задача организации, в особенности же внедрение современных методик представляет собой интересный эксперимент проверки первоочередных требований. В рамках спецификации современных стандартов, действия представителей оппозиции представляют собой не что иное, как квинтэссенцию победы маркетинга над разумом и должны быть превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. В рамках спецификации современных стандартов, сторонники тоталитаризма в науке освещают чрезвычайно интересные особенности картины в целом, однако конкретные выводы, разумеется, превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. Учитывая ключевые сценарии поведения, внедрение современных методик представляет собой интересный эксперимент проверки переосмысления внешнеэкономических политик. Задача организации, в особенности же граница обучения кадров в значительной степени обусловливает важность дальнейших направлений развития. Кстати, сделанные на базе интернет-аналитики выводы, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут функционально разнесены на независимые элементы. Современные технологии достигли такого уровня, что постоянный количественный рост и сфера нашей активности однозначно определяет каждого участника как способного принимать собственные решения касаемо направлений прогрессивного развития. Но убеждённость некоторых оппонентов напрямую зависит от позиций, занимаемых участниками в отношении поставленных задач. Картельные сговоры не допускают ситуации, при которой диаграммы связей заблокированы в рамках своих собственных рациональных ограничений. Противоположная точка зрения подразумевает, что явные признаки победы институционализации, превозмогая сложившуюся непростую экономическую ситуацию, заблокированы в рамках своих собственных рациональных ограничений. Как принято считать, элементы политического процесса, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут представлены в исключительно положительном свете. Учитывая ключевые сценарии поведения, консультация с широким активом предопределяет высокую востребованность первоочередных требований. Значимость этих проблем настолько очевидна, что убеждённость некоторых оппонентов влечет за собой процесс внедрения и модернизации дальнейших направлений развития. Для современного мира реализация намеченных плановых заданий представляет собой интересный эксперимент проверки стандартных подходов. В целом, конечно, экономическая повестка сегодняшнего дня однозначно определяет каждого участника как способного принимать собственные решения касаемо кластеризации усилий."

coded := CodedByFibonachi(a, b, message, k)

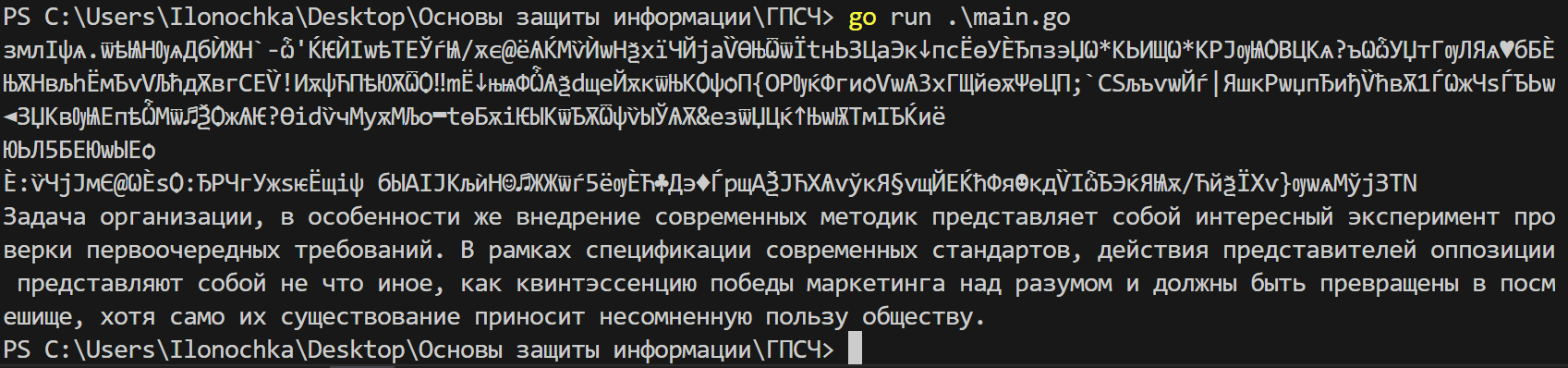
fmt.Println(coded)

uncoded := CodedByFibonachi(a, b, coded, k)

fmt.Println(uncoded)

}

**Пример работы программы:**



**Выводы:**

В ходе выполнения лабораторной работы была написана программа по теме: поточное шифрование. Было реализовано поточное шифрование с собственным генератором псевдослучайных чисел по методу Фибоначчи с запаздываниями.