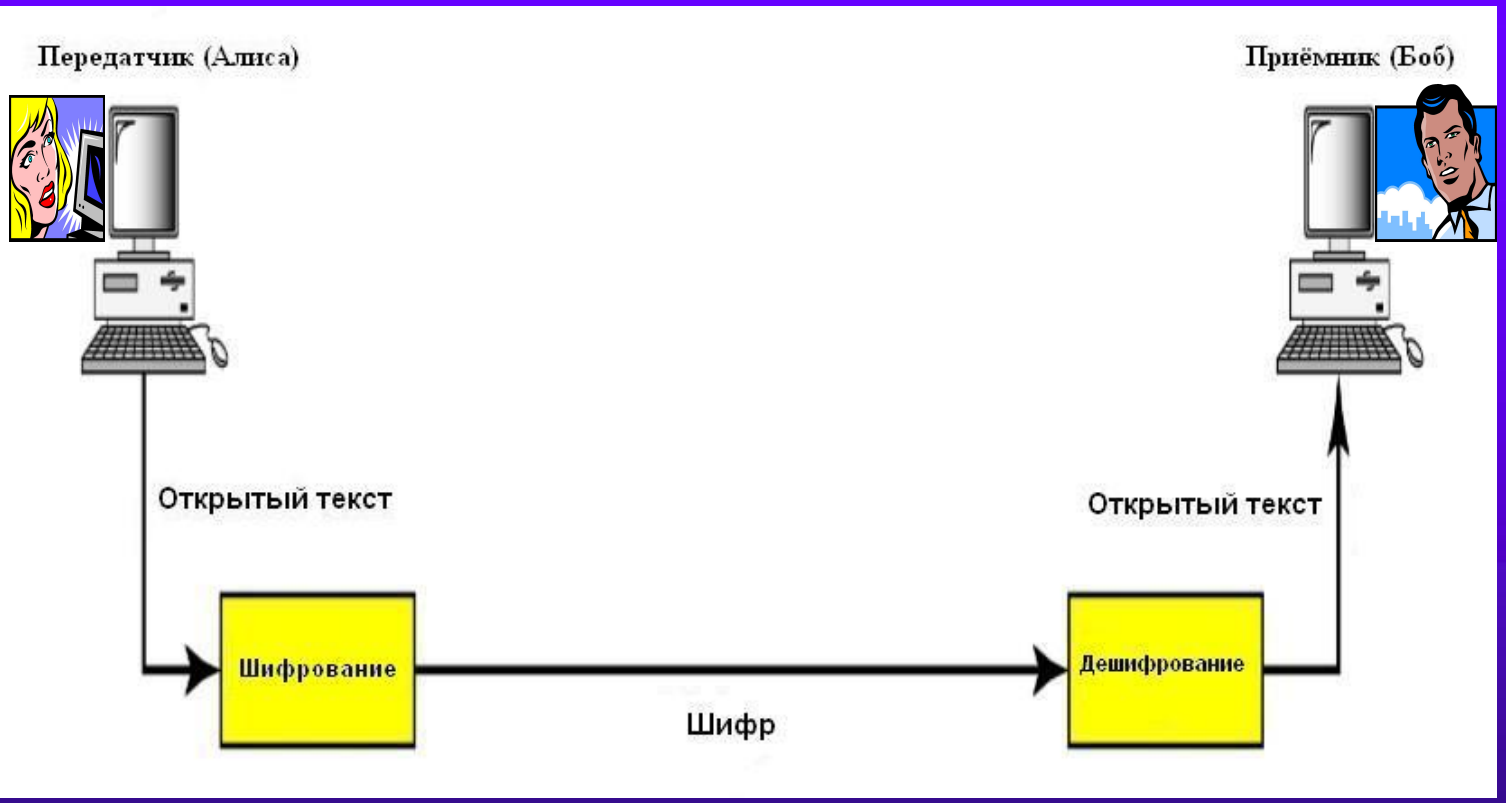
МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БАШКОРТОСТАН
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
КУШНАРЕНКОВСКИЙ МНОГОПРОФИЛЬНЫЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ

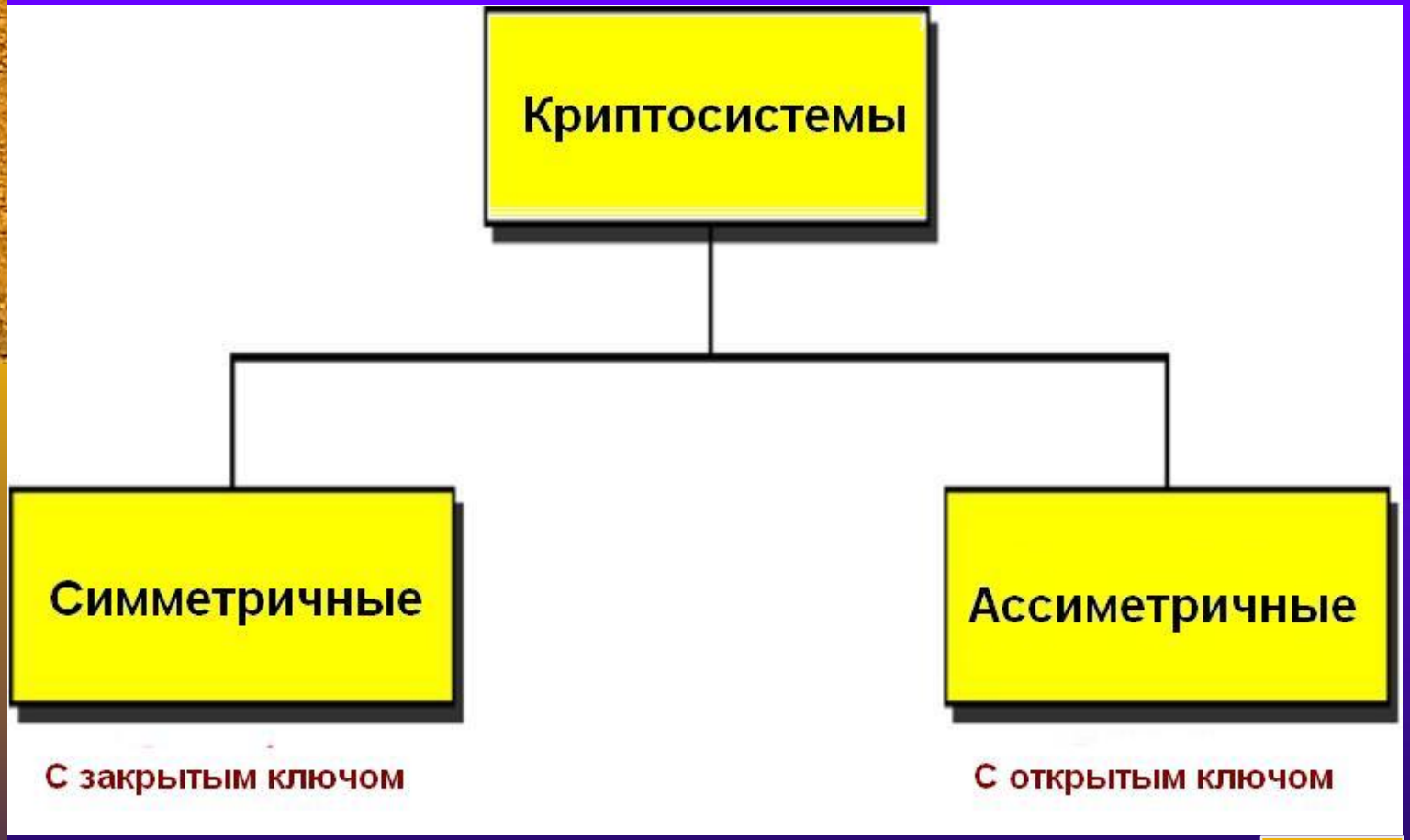
Криптографические методы защиты информации

Содержание

Основная схема криптографии



Категории криптографии



Ключи, используемые в криптографии

Симметричные криптосистемы

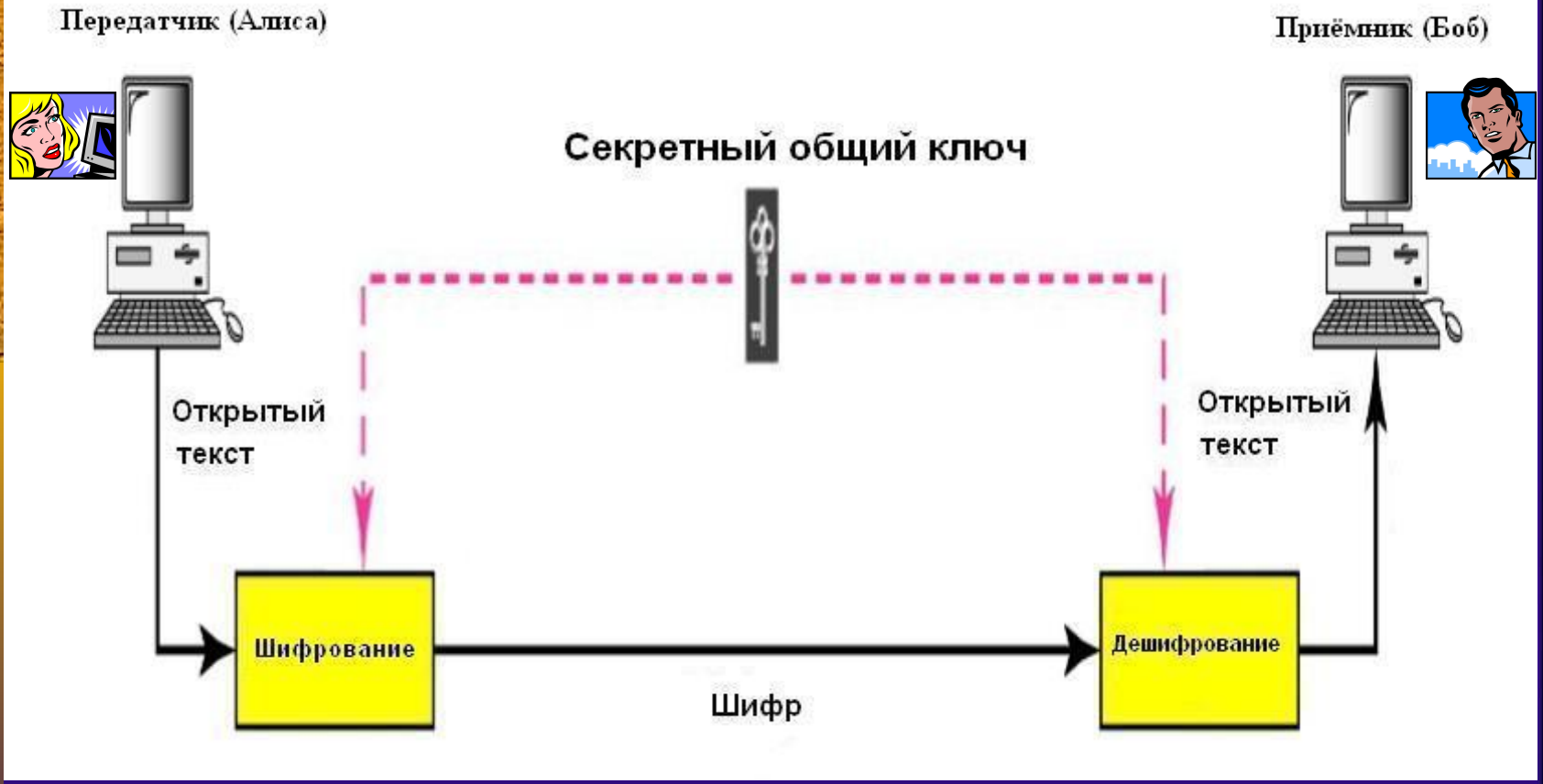
Асимметричные криптосистемы

Шенноновская теория секретности

- **Теорема Шеннона:** Для того, чтобы криптографическая схема была абсолютно секретной, *секретный ключ должен быть случайным и длина ключа должна быть по крайней мере равна длине открытого текста.*

Клод Шеннон

Симметричные криптосистемы



Симметричные криптосистемы: трудности

- Для шифрования и дешифрования используется ***общий ключ.***
- И передатчик, и получатель должны знать общий ключ.
- Общий ключ должен быть передан по второму секретному каналу связи.
- Создание и передача длинного секретного ключа.
- Непрактичны для большого числа передатчиков и получателей.

Известные симметричные криптосистемы

- Известные симметричные криптосистемы с : DES, AES.
- DES: разработан фирмой IBM для правительства США. Национальный стандарт шифрования США в 1977-2000 годах.
- AES: создан Дейманом и Рейманом в Бельгии. Национальный стандарт шифрования США с 2000 года.

Симметричные криптосистемы: примеры

- **Шифр Цезаря:** построен по алгоритму: читать четвертую букву вместо первой, т.е. ключ равен 3.
- В шифре Цезаря ключ равен 3 (величине сдвига букв алфавита).

Пример:

- Открытый текст: **meet me at central park**
- Шифр: phhw ph dw fhqwudo sdun

Недостаток криптосистемы: легко можно раскрыть шифр

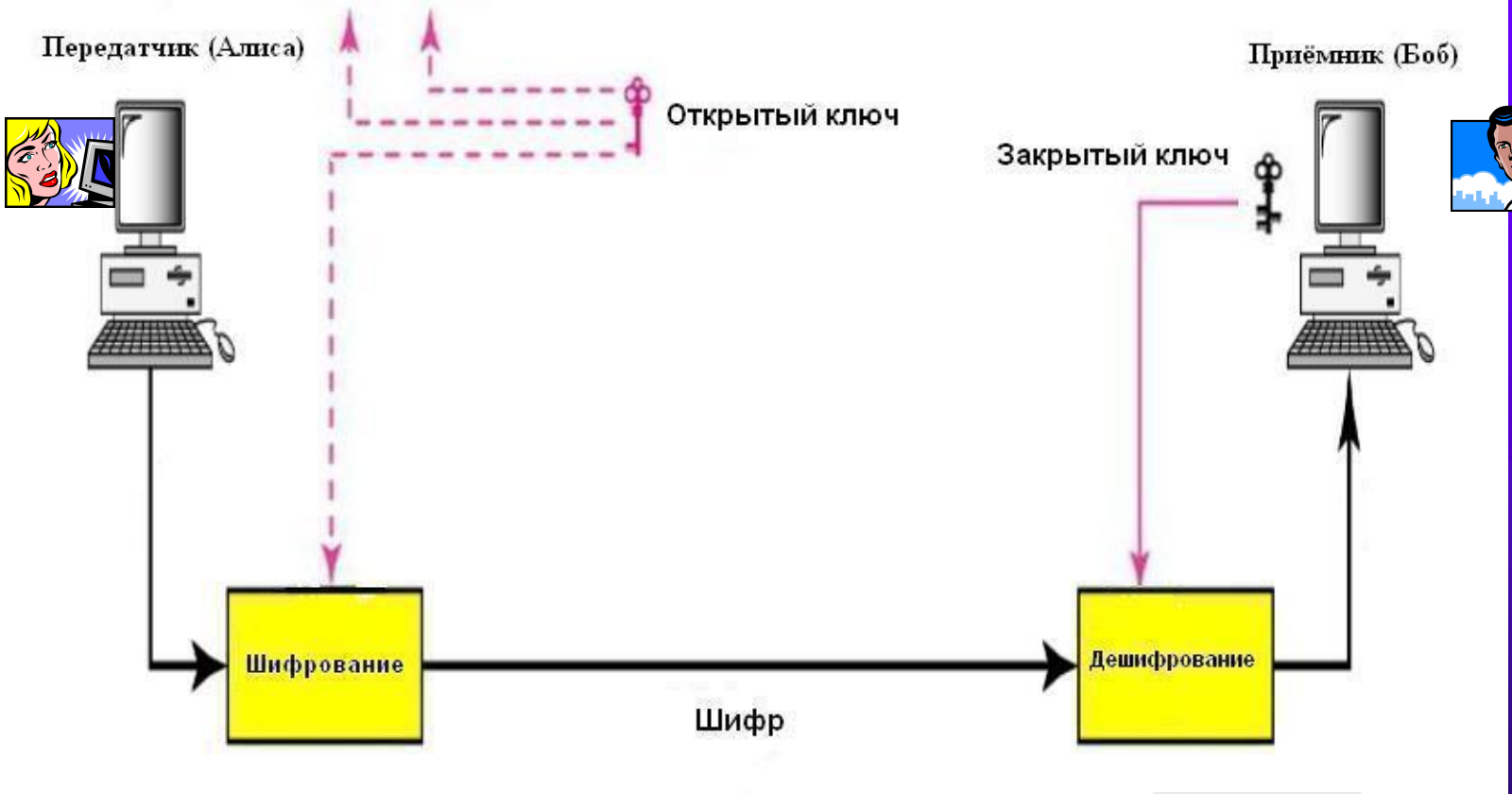
Симметричные криптосистемы: шифр Виженера

- записать под последовательностью цифр открытого текста последовательность цифр ключа, при этом последовательность цифр ключа записать необходимое число раз,
- сложить попарно эти две последовательности, при этом если сумма равна или больше 26, то вычесть 26.
- Заменить полученные цифры буквами английского языка согласно пункту 1.

Симметричные криптосистемы: шифр Виженера

- Согласно алгоритму ключ *cipher* заменяется последовательностью цифр (2,8,15,7,4,17),
- согласно алгоритму открытый текст *meet me at central park* заменяется последовательностью цифр (12,4,4,19,12,4,0,19,2,4,13,19,17,0,11,15,0,17,10),
- в качестве шифра исходного открытого текста получим последовательность *omtaqvcbrlrmtiaweim*.

Асимметричные криптосистемы



Асимметричные криптосистемы

- Идея *асимметричных криптосистем* впервые была предложена в 1976 году Диффи и Хеллманом на национальной компьютерной конференции как способ решения указанных выше трудностей симметричных криптосистем.
- Это одно из важных изобретений в истории секретной коммуникации:

Меркли, Хеллман, Диффи

Асимметричные криптосистемы: основные идеи

Приёмник (Боб):

- публикует свой открытый ключ и алгоритм шифрования,
- сохраняет в секрете соответствующий секретный ключ.

Передатчик (Алиса):

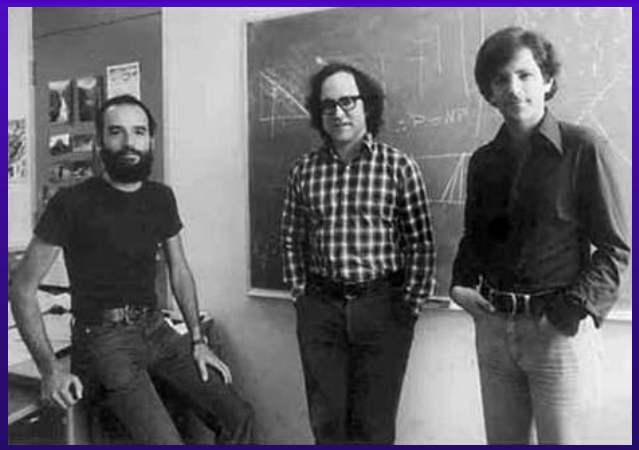
- из справочника берёт открытый ключ и алгоритм шифрования Боба,
- шифрует сообщение, используя открытый ключ и алгоритм шифрования Боба,
- посылает шифр Бобу.

Асимметричные криптосистемы: основные свойства

- Для шифрования и дешифрования используются *различные ключи.*
- Для шифрования сообщений используется *открытый ключ,* являющийся общедоступным.
- Для дешифрования сообщений используется *закрытый ключ,* являющийся секретным.
- Знание открытого ключа не даёт возможность определить закрытый ключ.

Известные асимметричные криптосистемы

- Известные криптосистемы с открытым ключом: ***RSA, ElGamal, McEliece.***
- ***Криптосистема RSA*** (создатели: Р. Ривест, А. Шамир и Л. Адлеман(1977 г.)) – одна из надёжных криптосистем.



Шамир, Ривест и Адлеман

Заключение

В этой теме я узнал что в криптографии бывают два категории Симметричные и Ассиметричные. Так же я узнал что идея *асимметричных криптосистем* впервые была предложена в 1976 году Диффи и Хеллманом на национальной компьютерной конференции как способ решения трудностей симметричных криптосистем .Это одно из важных изобретений в истории секретной коммуникации. **Теорема Шеннона:** Для того, чтобы криптографическая схема была абсолютно секретной, *секретный ключ должен быть случайным и длина ключа должна быть по крайней мере равна длине открытого текста.* Известные криптосистемы с открытым ключом: ***RSA, ElGamal, McEliece.***

Криптосистема RSA (создатели: Р. Ривест, А. Шамир и Л. Адлеман(1977 г.)) – одна из надёжных криптосистем

Список литературы

1. Методические указания по выполнению и темы курсовых работ по дисциплине “Информатика” ВЗФЭИ, 2006.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. - М.: 2005. - 480с.
3. Введение в криптографию /Под общ. ред. В. В. Ященко --- М., МЦНМО, 1998, 1999, 2000 - 272 с.
4. Герасименко В.А., Малюк А.А. Основы защиты информации: Учебник для вузов. М.: Изд-во ООО «Инкомбанк», 1997.
5. Панасенко С.П., Защита информации в компьютерных сетях // Журнал «Мир ПК» 2002 № 2.

Список литературы

- 6. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия.-СПб.: БХВ-Петербург, 2003.- 752с.:ил.
- 7. Мелюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. -М.: Горячая линия - Телеком, 2001.- 48с.:ил.
- 8. Оглтри Т. Практическое применение межсетевых экранов: Пер. с англ.-М.: ДМК Пресс, 2001.- 400с.:ил.
- 9. Сетевые операционные системы/ В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2002. – 544с.: ил.
- 10. Соколов А. В., Степанюк О. М. Защита от компьютерного терроризма. Справоч-ное пособие. - СПб.: БХВ - Петербург, Арлит, 2002.- 496с.:ил.