Криптографические методы защиты информации

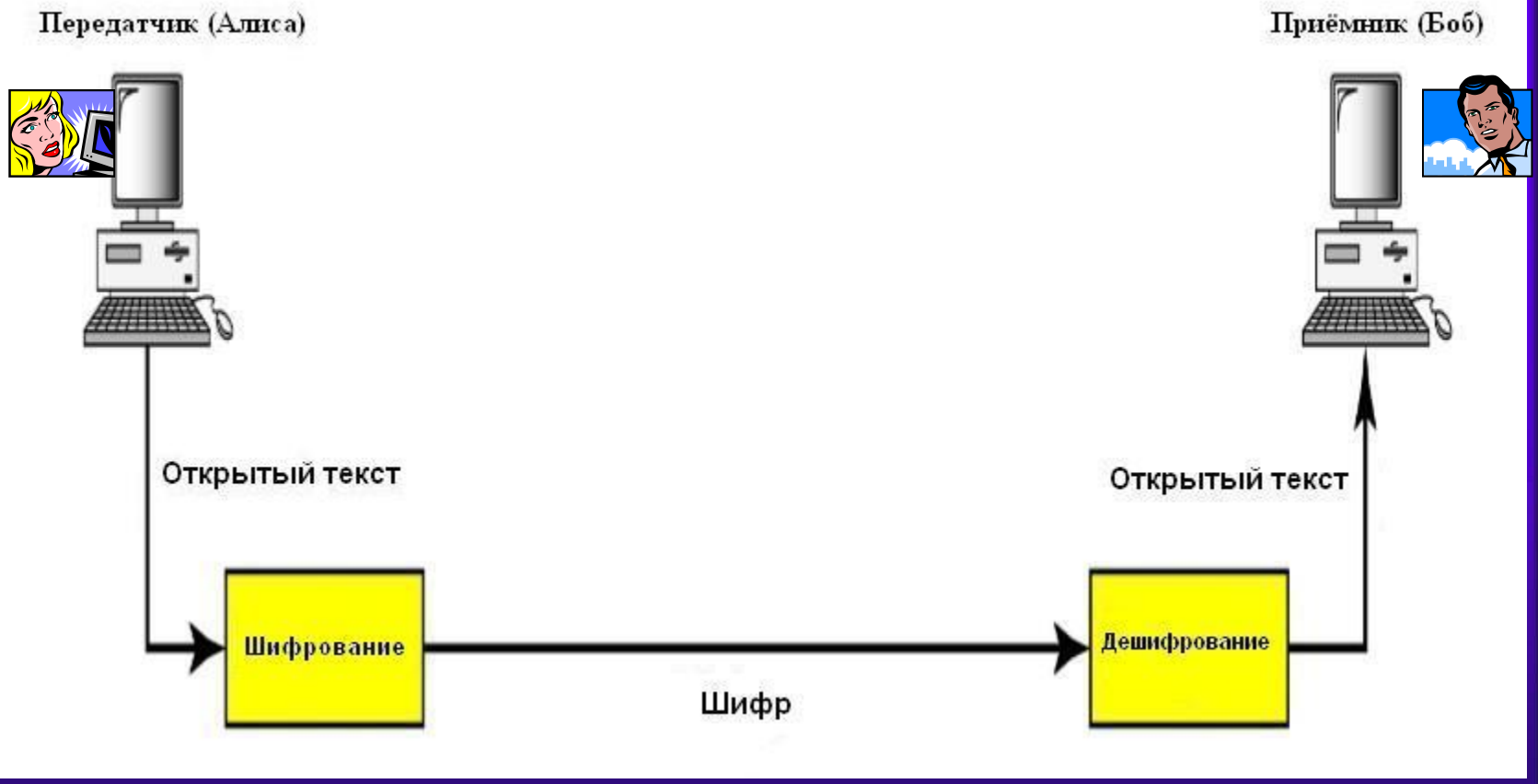
• **Криптология** — наука о защите информации – делится на две части: **криптографию** и **криптоанализ.**

• **Криптография** – это часть криптологии, связанная с проектированием секретных систем.

•**Криптоанализ** – это часть криптологии, связанная со взломом секретных систем.

- *Криптограф* ищет методы, обеспечивающие секретность и/или подлинность информации путём шифрования исходного текста.
- *Криптоаналитик* пытается выполнить обратную задачу, раскрывая шифр или подделывая сообщение так, чтобы выдать их за подлинные.

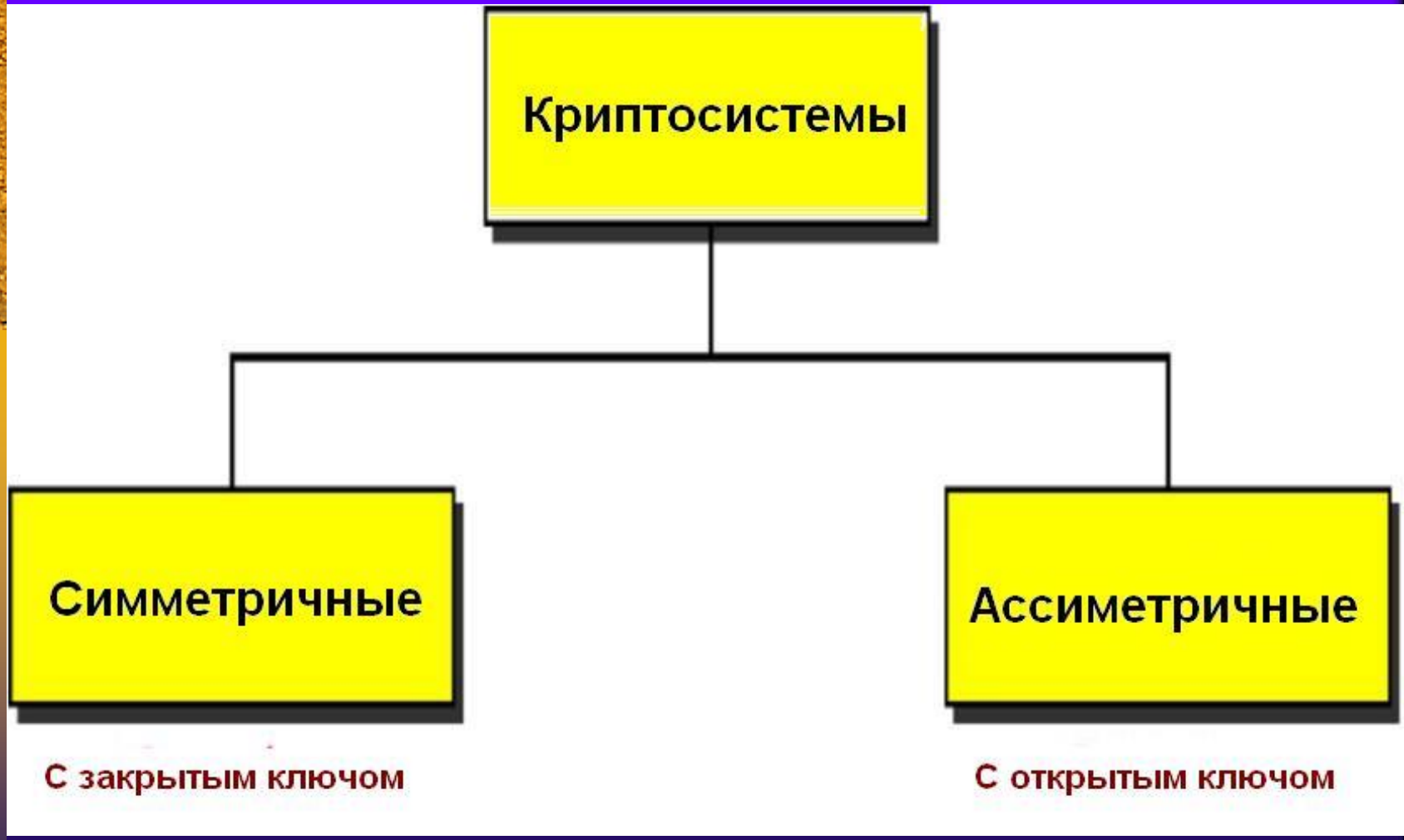
Основная схема криптографии



Основная схема криптографии

- ***Криптографическая схема называется абсолютно секретной***, если знание шифра не даёт информации об открытом тексте.
- **Задача состоит в построении абсолютно секретных криптографических схем.**

Категории криптографии



Ключи, используемые в криптографии

Симметричные криптосистемы

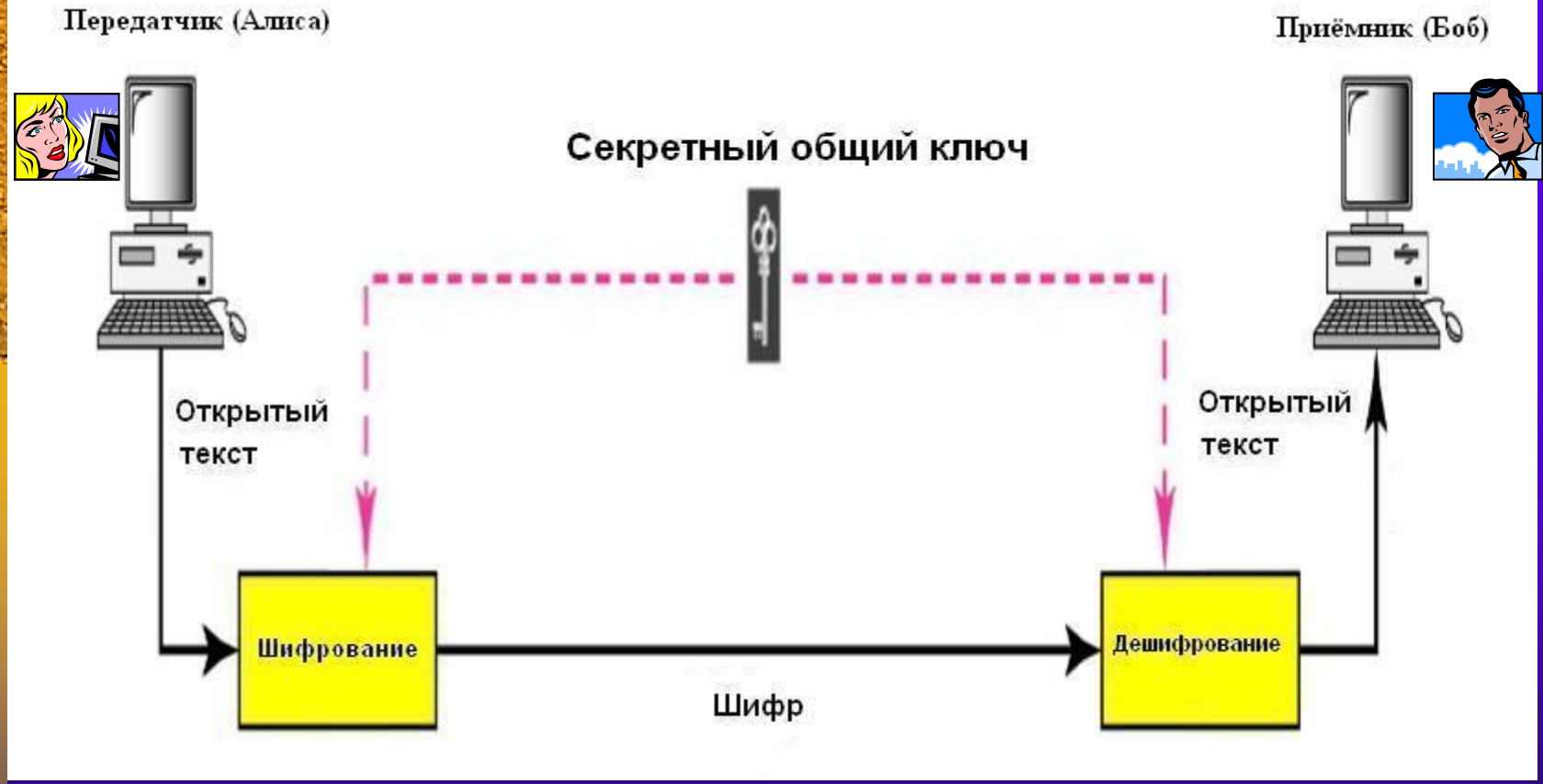
Асимметричные криптосистемы

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.

Симметричные криптосистемы: достоинства

- Простота и быстрота построения и реализации.
- Высокое быстродействие.
- Все классические криптосистемы симметричные.

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: примеры

Шифр Виженера: построен по следующему алгоритму:

- заменить каждую букву английского языка цифрой 0-25: A $\leftrightarrow$ 0, B $\leftrightarrow$ 1, …, Z $\leftrightarrow$ 25,
- в качестве ключа рассмотреть любую последовательность букв английского языка,
- заменить ключ последовательностью цифр согласно пункту 1,
- заменить открытый текст последовательностью цифр согласно пункту 1,

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

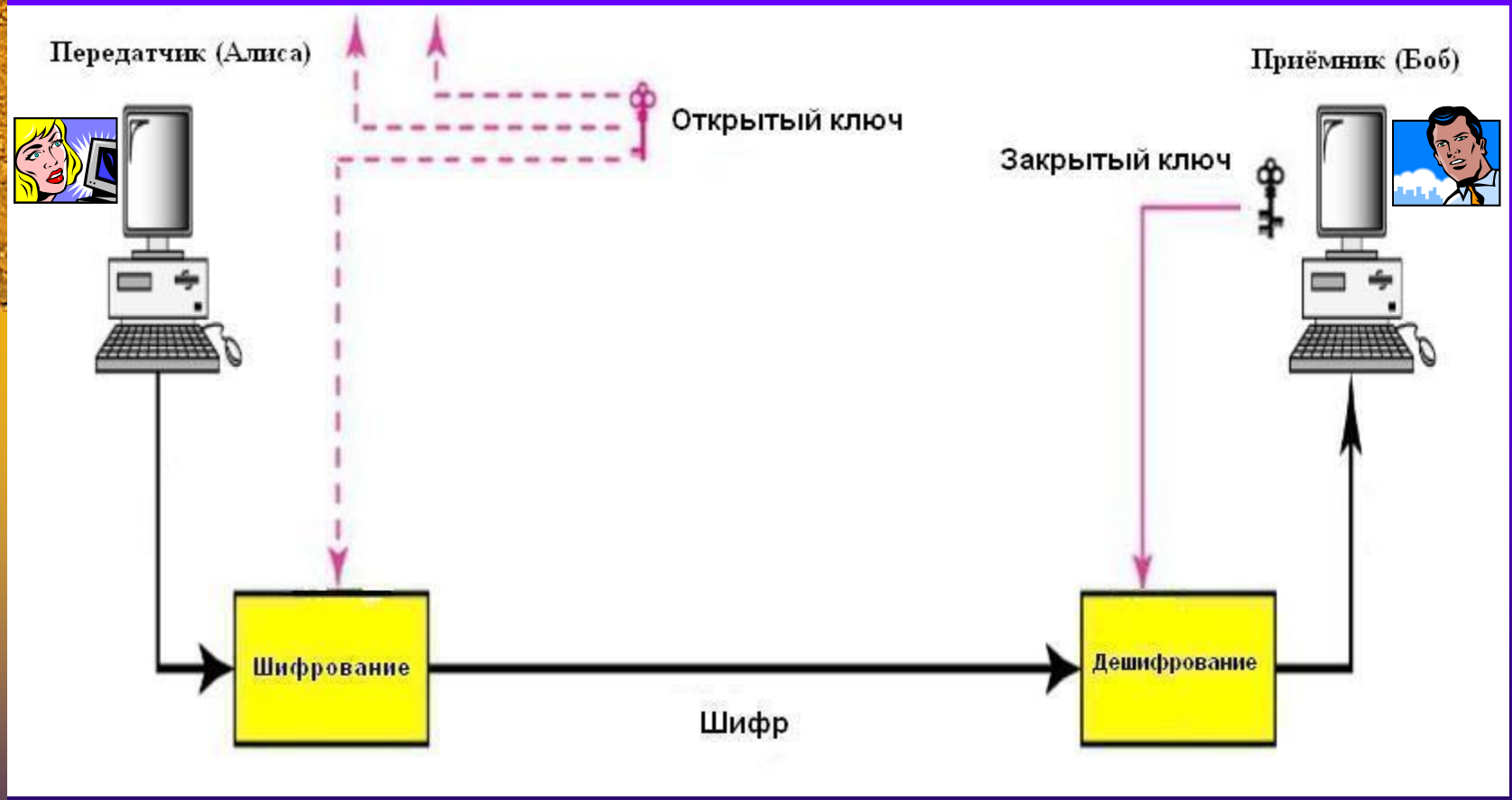
Пример:

- Открытый текст: **meet me at central park**
- Ключ: **cipher**

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 идеи

Приёмник (Боб):

- получает шифр от передатчика (Алисы),
- дешифрует шифр, используя свой секретный ключ и алгоритм дешифрования.

Асимметричные криптосистемы: основные свойства

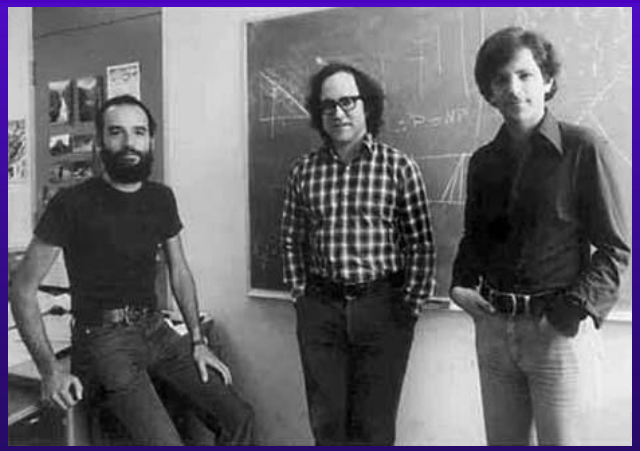
- Для шифрования и дешифрования используются *различные ключи.*
- Для шифрования сообщений используется *открытый ключ,* являющийся общедоступным.
- Для дешифрования сообщений используется *закрытый ключ,* являющийся секретным.
- Знание открытого ключа не даёт возможность определить закрытый ключ.

Асимметричные криптосистемы: достоинства

- Не требуется секретный общий ключ.
- Простая схема обеспечения секретности (не требуется доверяемая третья сторона).
- Удобна для защиты информации в открытой многопользовательской среде.

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