Симметричное и ассиметричное шифрование

Преподаватель:
Петелин Александр Евгеньевич

Ключ (*криптографический ключ*) – специальный информационный объект (обычно представленный в виде набора букв, цифр и символов), который реализуют доступ к шифрованию/дешифрованию.

Открытый ключ – ключ, который может быть известен посторонним лицам. Как правило, открытый ключ передается между участниками по ***открытому каналу*** (то есть незащищённому, доступному для наблюдения).

Закрытый ключ (*секретный ключ*) – ключ, который может быть известен только ограниченному кругу лиц.

Шифрование – способ преобразования открытой информации в закрытую и обратно. Шифрование подразделяется на процесс зашифровывания и расшифровывания.
Дешифрование – получение открытых данных по зашифрованным в условиях, когда алгоритм расшифрования не является полностью (вместе со всеми секретными параметрами) известным и расшифрование не может быть выполнено обычным путем (процесс обратный процессу шифрования).

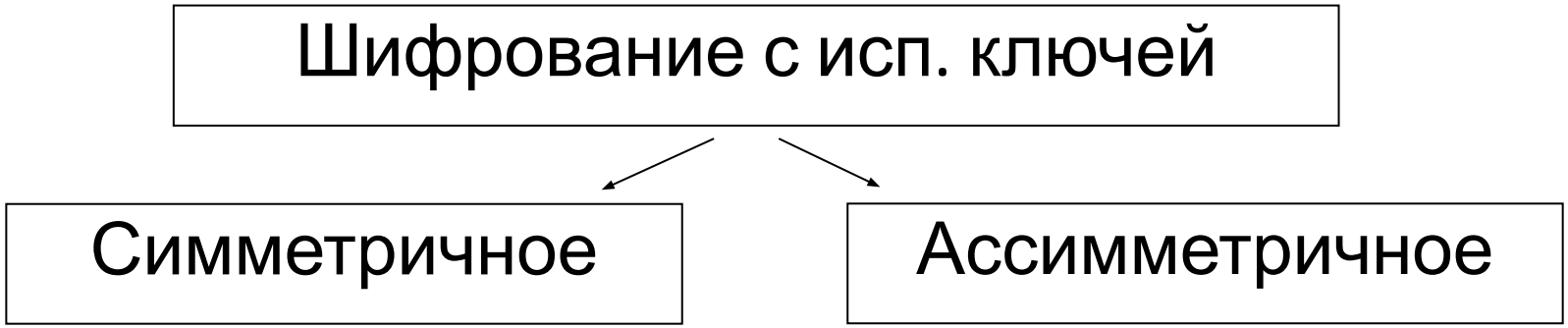
Криптоанализ – набор методов и средств для выполнения (или сам процесс) дешифрования информации без обладания необходимым ключом.

Методы шифрования:

шифрование заменой (подстановка) – символы шифруемого текста заменяются другими символами (например, буква А заменяется буквой м, Б заменяется л и т. д.);

шифрование перестановкой (например, Стул можно зашифровать как Тслу),

шифрование с использованием ключей.



Симметричное шифрование (*или симметричные криптосистемы, симметричные шифры*) – способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ, который должен сохраняться в секрете обеими сторонами, а алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Виды симметричных шифров:

1) ***блочные шифры*** (информация шифруется блоками из нескольких бит): DES, 3DES, AES, RC2, RC5, Blowfish, Twofish, NUSH, ГОСТ 28147-89, IDEA, CAST, CRAB, 3-WAY, KHUFU и KHAFRE;
2) ***потоковые шифры*** (зашифрован может быть каждый бит информации отдельно): RC4, SEAL, WAKE.

Симметричные шифры

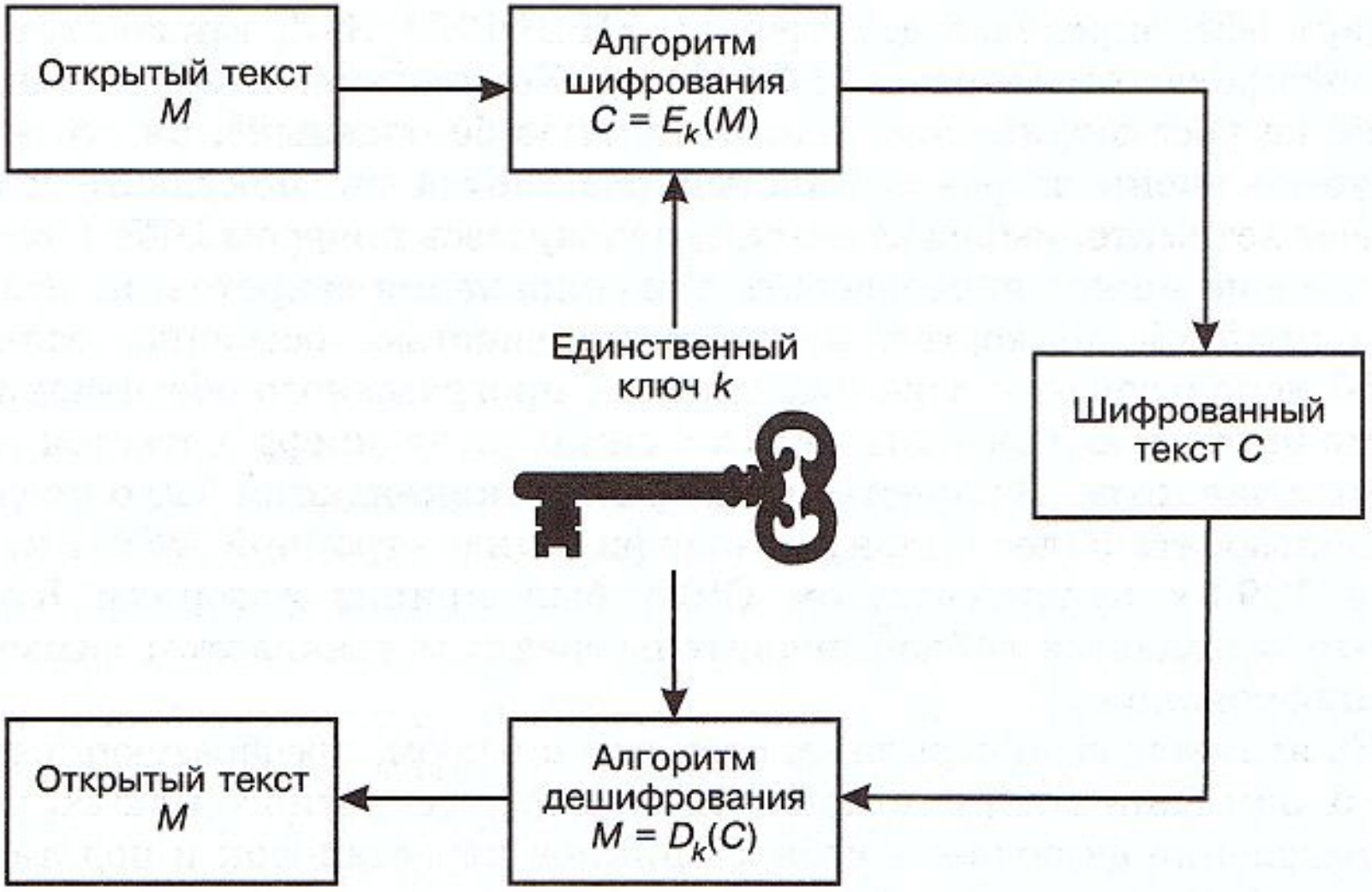
Преимущества:

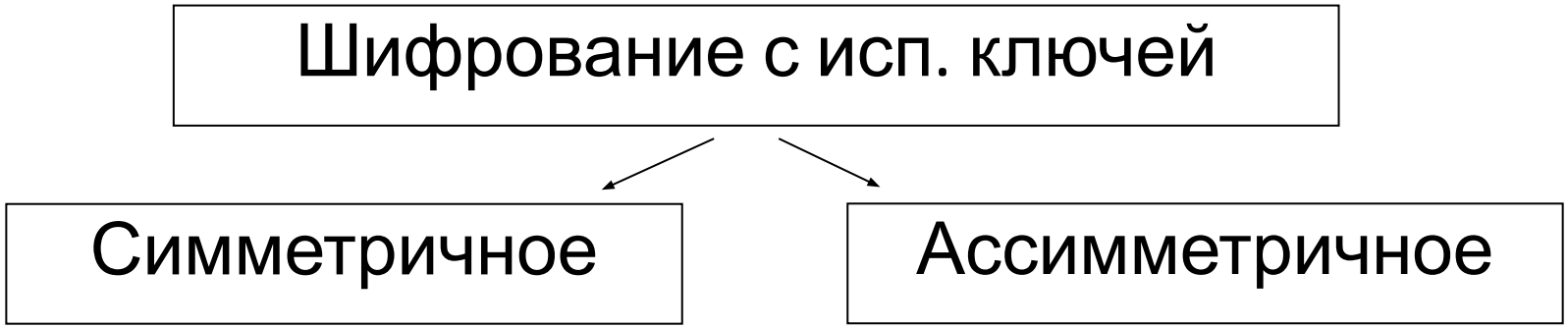
1) скорость (на 3 порядка быстрее асимметр.),
2) простота реализации (за счёт более простых операций),
3) меньшая требуемая длина ключа для сопоставимой стойкости,
4) изученность (за счёт большего возраста).

Недостатки:

1) сложность управления ключами в большой сети (большое их число),
2) сложность обмена ключами.

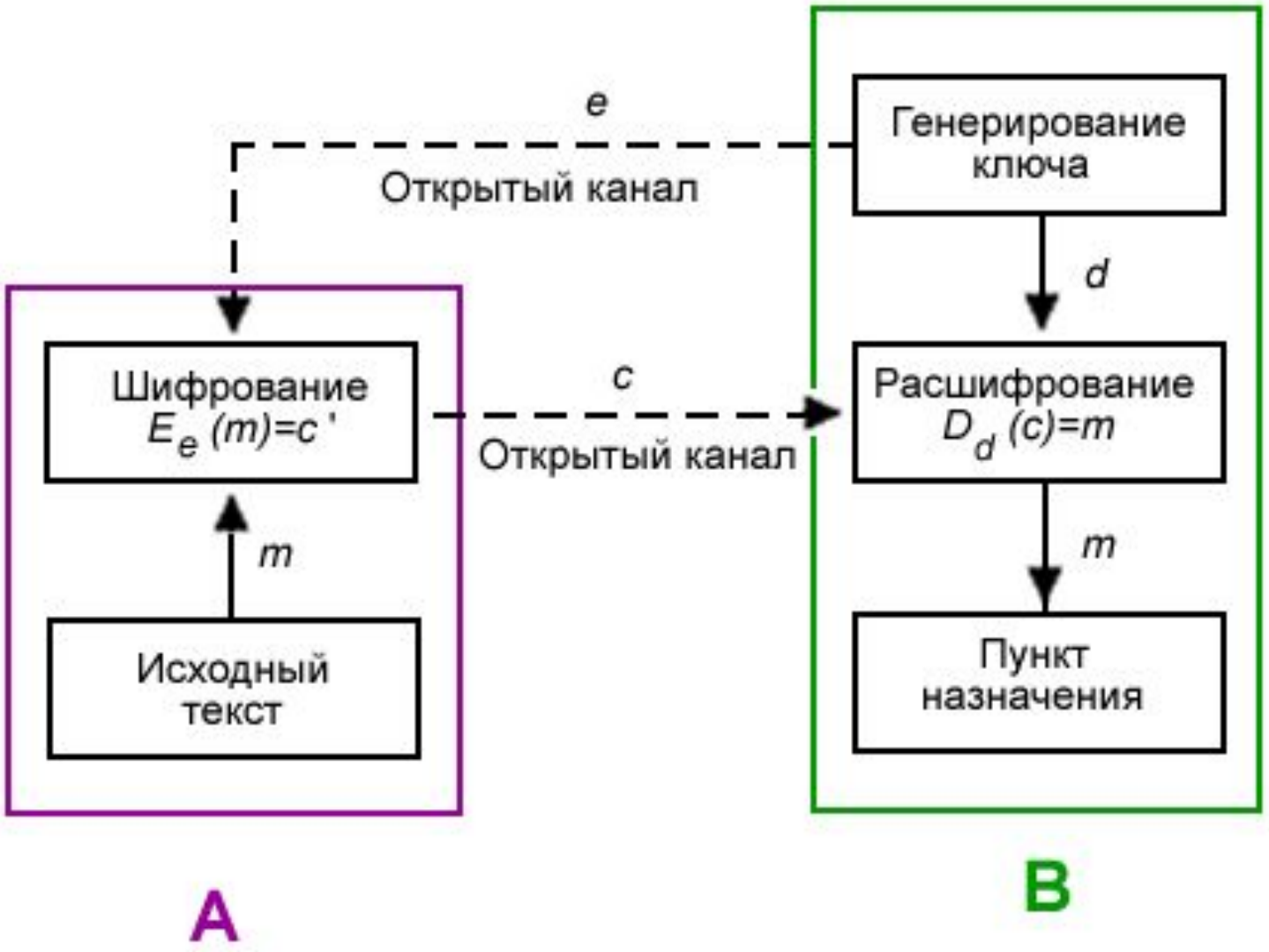
Схема шифрования





Асимметричное шифрование (*или криптографическая система с открытым ключом, асимметричный (несимметричный) шифр*) – способ шифрования, в котором для шифрования сообщения используется открытый ключ, а для расшифрования используется секретный ключ.

Схема шифрования



Асимметричные шифры

Недостатки:

1) довольно сложно внести изменения в алгоритм шифрования;
2) много пересылок сообщений (помимо шифротекста необходимо пересылать открытый ключ);
3) используются более длинные ключи (в 5–10 раз больше);
4) менее производительно (медленнее);
5) требуют больших вычислительных ресурсов.

Асимметричные шифры

Преимущества:

1) нет необходимости передавать ключи по надежному каналу связи;
2) закрытый ключ держится в секрете только одной стороной;
3) ключи можно не менять значительное время;
4) значительно меньшее количество ключей.

Виды асимметричных шифров:

RSA, DSA, Elgamal, Diffie-Hellman, ECDSA, ГОСТ Р 34.10-2001, Rabin, Luc, McEliece, Williams System.