Государственное профессиональное образовательное учреждение
Тульской области
«Тульский технико-экономический колледж имени А.Г.Рогова»

Проект
по дисциплине: «Информатика»
На тему: «Шифрование с использованием закрытого ключа»

Выполнил: студент группы 1-1
Савенков Станислав Сергеевич
Принял преподаватель:
Зеленцова Ольга Анатольевна

Тула 2019 год

ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ

В целом:

E (p, открытый r) = зашифрованный текст p

D (зашифрованный p, закрытый r) = текст p


Методы шифрования с закрытым ключом
Замена
Перестановка
Комбиниро-ванные
Другие
Одно-алфавитная
Много-алфавитная
Простая (с фиксированным периодом)
Табличная
Усложненная по маршрутам
Блочные шифры
Поточные шифры
Смысловое
Сжатие/ расширение
Примеры методов шифрования с закрытым ключом

Системы шифрования

(криптография)

Ключ – определяет алгоритм шифрования:

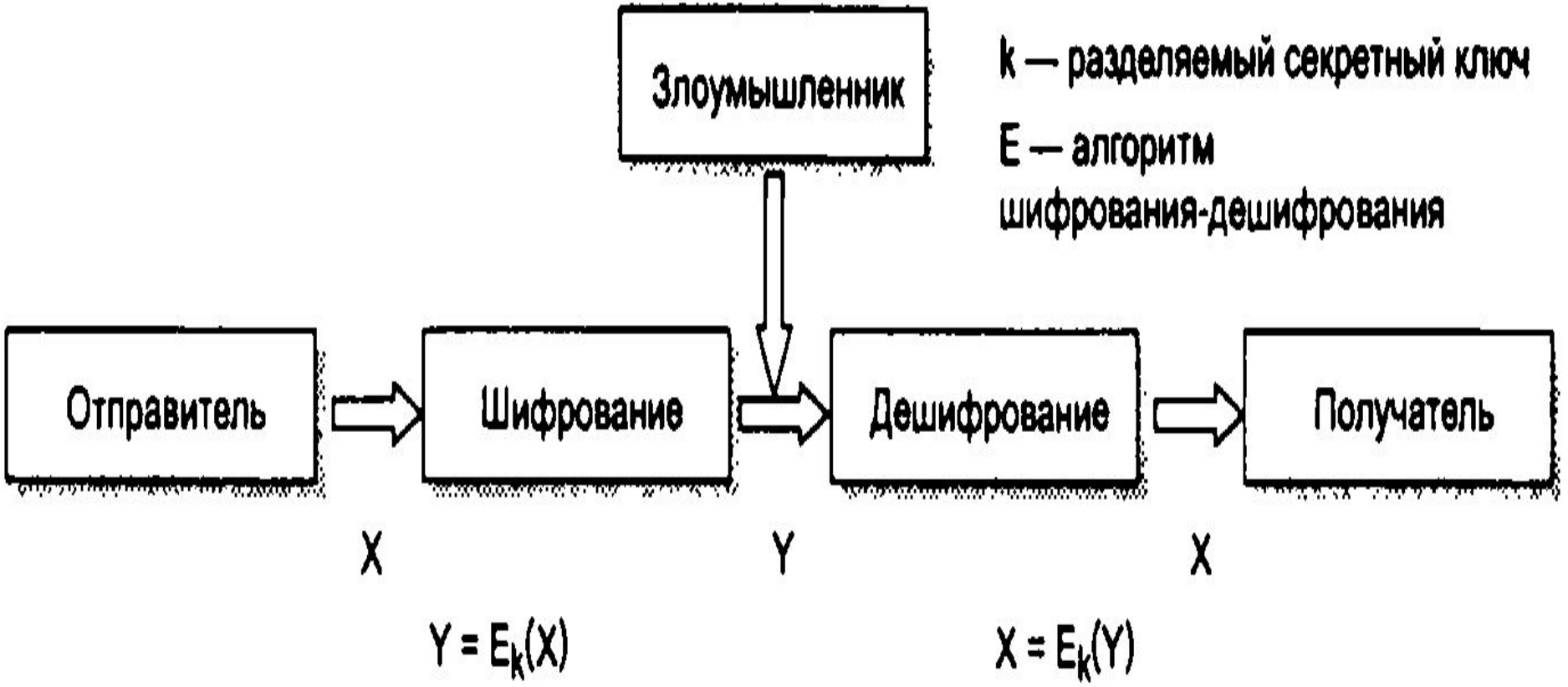
- **с закрытым ключом,** которым заранее обмениваются два абонента, ведущие секретную переписку, и сохраняемый в тайне от третьих лиц.
- **с открытым ключом** (асимметричный алгоритм), использует отдельно шифровальный (открытый) и дешифровальный (закрытый) ключей.

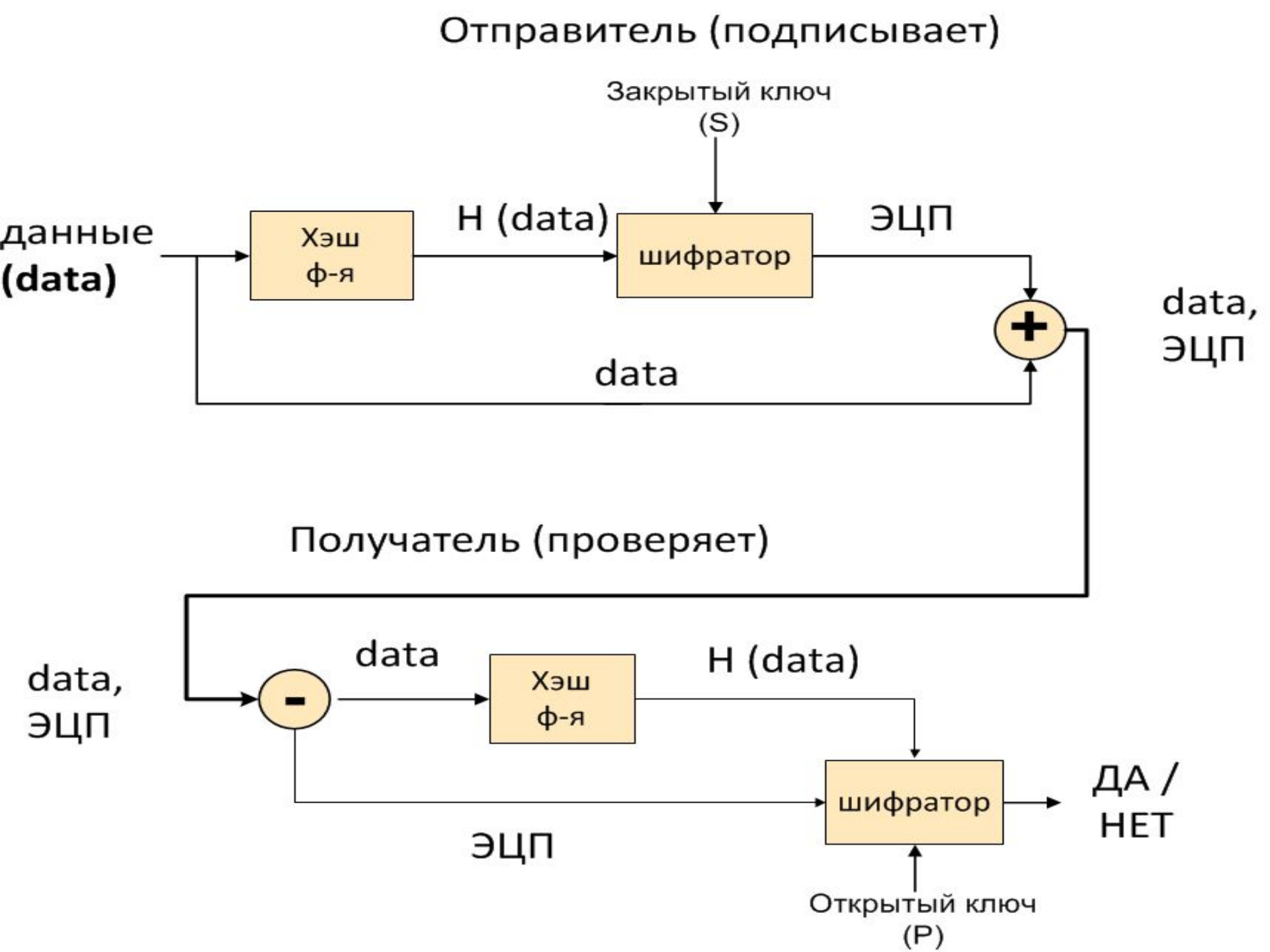
Системы шифрования

(криптография)

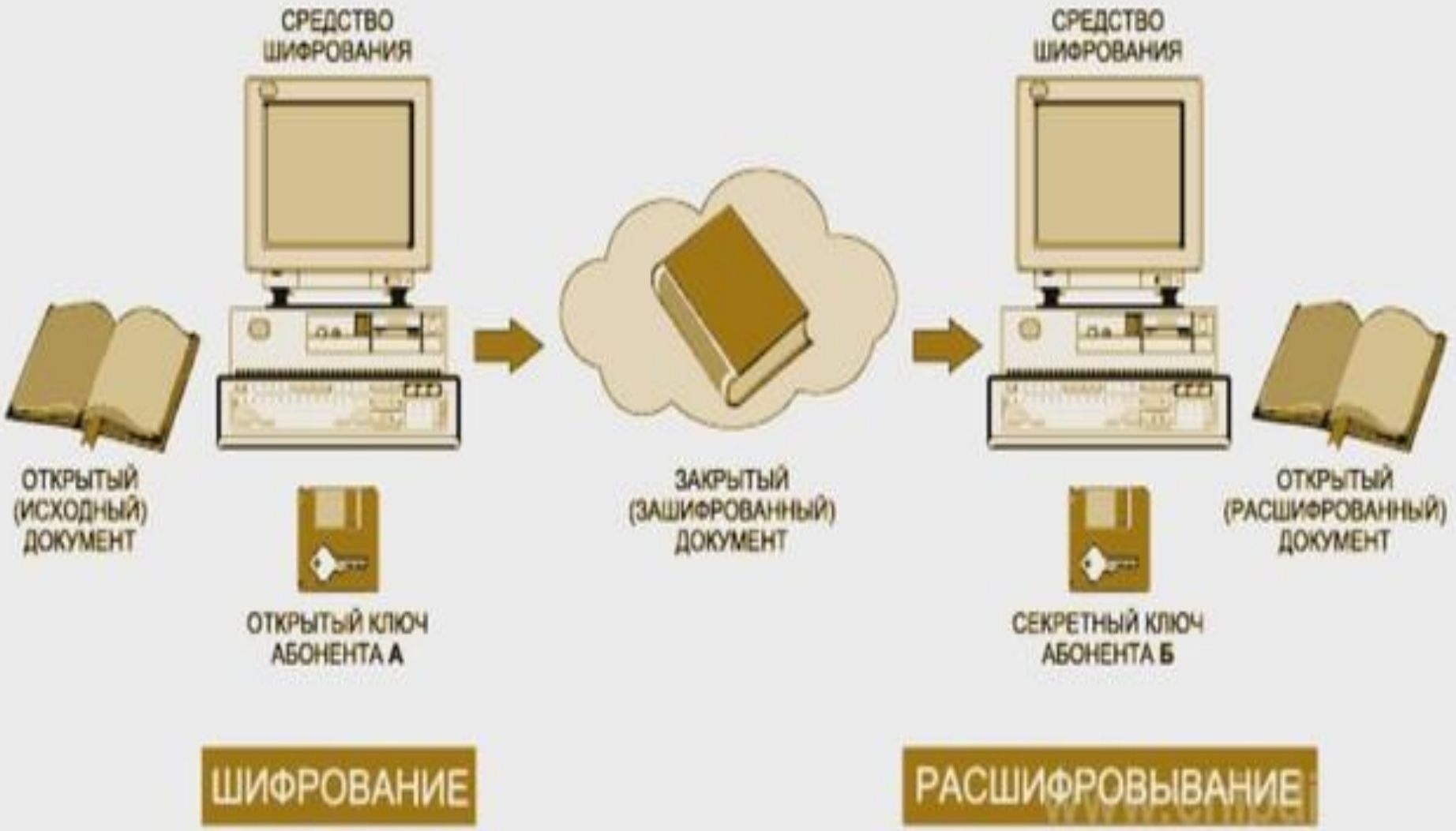
Ключ – определяет алгоритм шифрования:

- **с закрытым ключом,** которым заранее обмениваются два абонента, ведущие секретную переписку, и сохраняемый в тайне от третьих лиц.
- **с открытым ключом** (асимметричный алгоритм), использует отдельно шифровальный (открытый) и дешифровальный (закрытый) ключей.


Злоумышленник
k — разделяемый секретный ключ
E — алгоритм шифрования-дешифрования
Отправитель
Шифрование
Дешифрование
Получатель
X
Y
X
Y = Ek(X)
X = Ek(Y)


Отправитель (подписывает)
Закрытый ключ
(S)
данные
(data)
Хэш
ф-я
H (data)
шифратор
ЭЦП
+
data,
ЭЦП
data
Получатель (проверяет)
data,
ЭЦП
-
data
Хэш
ф-я
H (data)
шифратор
ДА /
НЕТ
ЭЦП
Открытый ключ
(P)

Асимметричный алгоритм шифрования



A problem has been detecetd and Windows has been shut down to prevent damage
to your computer.

DRAGONITE_HAS_NO_LIFE

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Actually, don't do anything. BSODs are good for your health.
(If you work for Apple, that is.)

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
Of course, you could simply not run anything else that Dragonite uploads to Wizirdi again.

Technical information:

*** STOP: 0.000000D1 (0x0000000C, 0x00000002, 0x00000000, 0x00001337)

***   trololo.sys - Address 1337000 base at 10101010, Datestamp 00000000

Begin dump of physical memory

Physical memory dump complete.
Contact your system administrator or technical support group for further