SCHOOL CTF

CRYPTO в CTF

ТИПЫ ЗАДАНИЙ

SCHOOL CTF

1. Расшифровать текст
2. Заставить сервер выплюнуть флаг (или как-то по другому извлечь информацию о флаге с сервера)
3. Подобрать пароль
4. ...

С ЧЕГО НАЧАТЬ?

- Анализ того, что дано
  - Описание таска и его основное содержание
  - Разобрать какие криптопримитивы используются и зачем
  - Попытаться понять, в чем состоит твоя задача
  - Если криптопримитив реализован, то сравнить реализацию со стандартом (в интернетах)

Что такое криптография?

Свойства информации, обеспечиваемые криптографией

- Конфиденциальность
- Целостность
- Аутентичность

Конфиденциальность

Конфиденциальность - секретность информации.
Обеспечивается с помощью шифров.
Шифр - пятерка (X, Y, K, E, D), где
X - множество открытых текстов,
Y - множество закрытых текстов,
K - множество ключей,
E: X x K -> Y,
D: Y x K -> X,
D(E(x)) = x.
Примеры: Одноалфавитная замена, Шифр Виженера, RC4, AES, RSA, ...

Целостность

Целостность информации - свойство информации, позволяющее проверять, находится ли информация в изначальном виде или нет. Обеспечивается с помощью хэш-функций, кодов аутентификации сообщений(MAC), цифровых подписей.

Аутентичность

Аутентичность информации - подлинность информации. Обеспечивается с помощью кодов аутентификации сообщений(MAC), цифровых подписей. Эти криптопримитивы обеспечивают некое доказательство принадлежности данных человеку или группе людей.

Хэш-функции

Хэш-функция - тройка (X, Y, H)

X - множество сообщений, имеют произвольную длину

Y - множество хэшей. Все хэши имеют фиксированную длину

H: X -> Y - функция

Для криптографии используются хэш-функции, обладающие свойствами:

1. Необратимость
2. Стойкость к коллизиям

Примеры: md5(уже нет), sha1, sha256, sha512

Одноалфавитная замена

X - множество текстов букв из алфавита A
Y - множество текстов букв из алфавита B
K - множество подстановок из A в B

E(x) = k(x), k принадлежит K

D(x) = k*(x), k* принадлежит K*, множеству подстановок из B в A

Одноалфавитная замена

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
CIPHERTEXT	U	D	I	E	F	G	H	Y	V	N	M	O	J	P	Q	A	C	B	T	S	W	R	K	L	Z	X

Sort alphabetically: Ciphertext | Plaintext

plaintext — Get Sample Message

well, prince, so genoa and lucca are now just family estates of the buonapartes. but i warn you, if you don't tell me that this means war, if you still try to defend the infamies and horrors perpetrated by that antichrist—i really believe he is antichrist—i will have nothing more to do with you and you are no longer my friend, no longer my 'faithful slave,' as you call yourself! but how do you do? i see i have frightened you—sit down and tell me all the news.

Encrypt

Decrypt

Clear All | Clear Messages

To Encrypt/Decrypt a Message

1. Put your message in the appropriate box.
2. Enter substitutions in the table.
3. Encrypt/Decrypt the first 3 letters.
4. Click Encrypt/Decrypt. We'll do the rest.

CIPHERTEXT — Get Sample Message

KFOO, ABVPIF, TQ HFPQU UPE OWIIU UBF PQK NWTS GUJVOZ FTSUSFT QG SYF DWQPUAUBSFT. DWS V KUBP ZQW, VG ZQW EQP'S SFOO JF SYUS SYVT JFUPT KUB, VG ZQW TSVOO SBZ SQ EFGFPE SYF VPGUJVFT UPE YQBBQBT AFBAFSBUSFE DZ SYUS UPSVIYBVTS—V BFUOOZ DFOVFRF YF VT UPSVIYBVTS—V KVOO YURF PQSYVPH JQBF SQ EQ KVSY ZQW UPE ZQW UBF PQ OQPHFB JZ GBVFPE, PQ OQPHFB JZ 'GUVSYGWO TOURF,' UT ZQW IUOO ZQWBTFOG! DWS YQK EQ ZQW EQ? V TFF V YURF GBVHYSFPFE ZQW—TVS EQKP UPE SFOO JF UOO SYF PFKT.

Аффинный шифр

Шифр Виженера

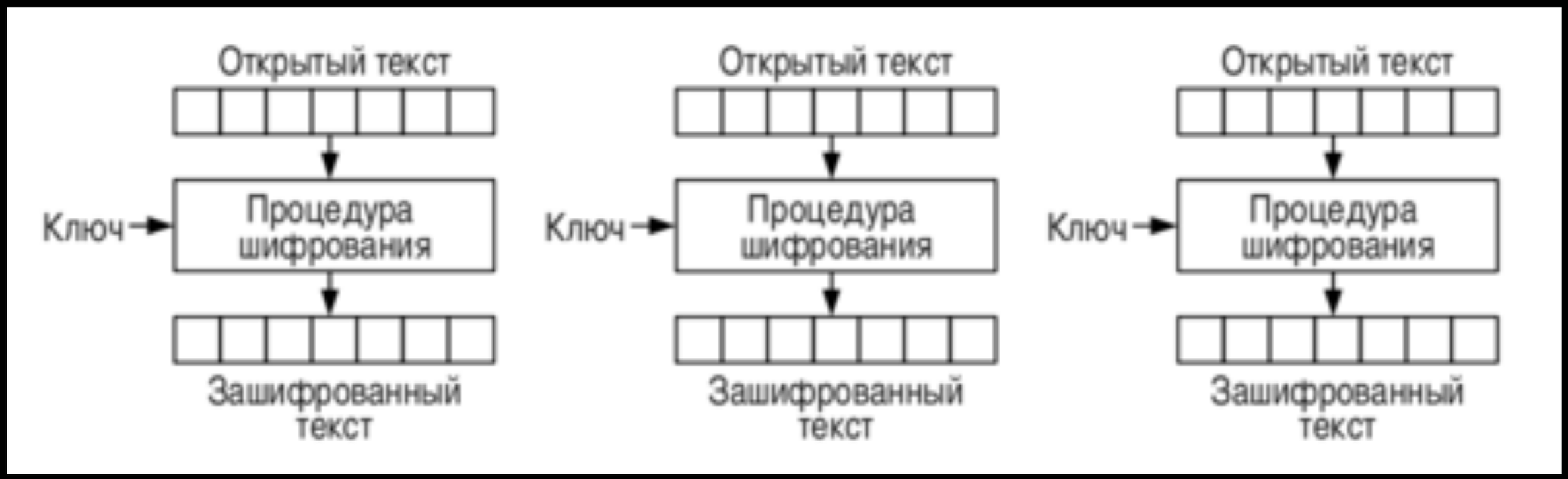
Другие шифры классической криптографии

Решетка Кардано, омофоническая замена, сцитала, столбцовая перестановка, ...

Подробнее - Сингх “Книга шифров”

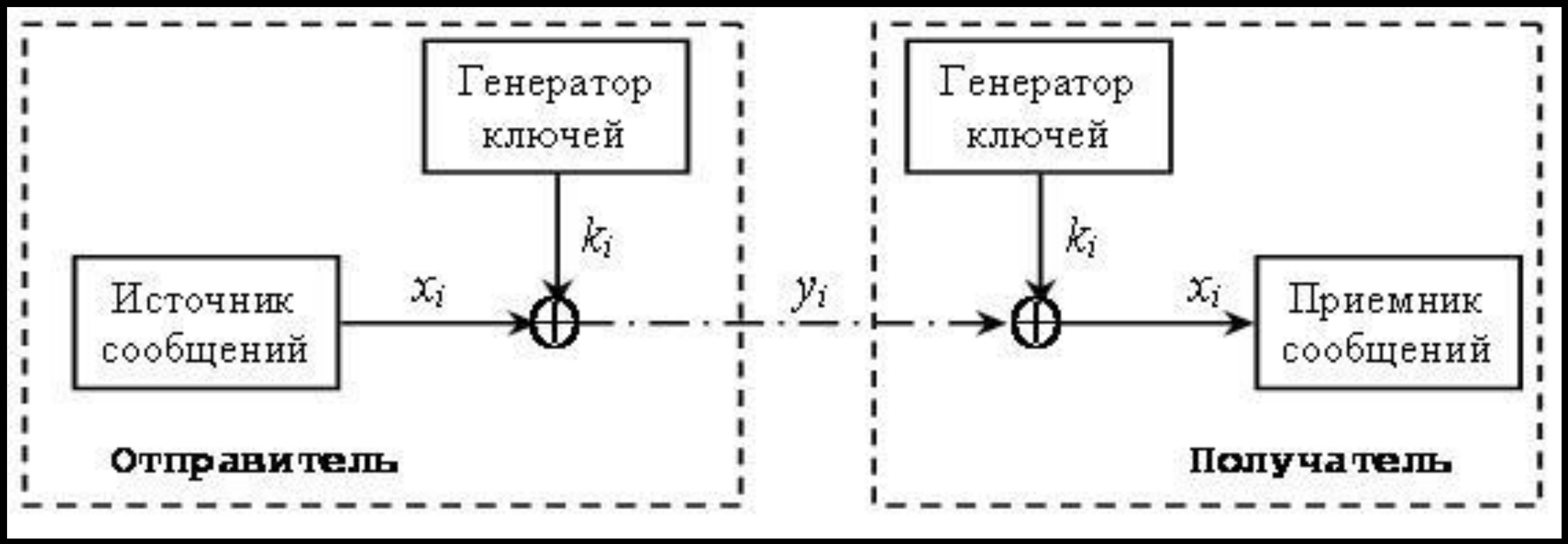
Блочные шифры

Блочные шифры - вид шифров, обрабатывающий за одну итерацию блок из нескольких байт.
Текст должен быть разделен на блоки одинаковой длины. Соответственно, длина текста должна быть кратна длине блоков. Для того, чтобы этому соответствовать используется padding.
Примеры шифров: AES, DES


Открытый текст
Ключ
Процедура шифрования
Зашифрованный текст
Открытый текст
Ключ
Процедура шифрования
Зашифрованный текст
Открытый текст
Ключ
Процедура шифрования
Зашифрованный текст

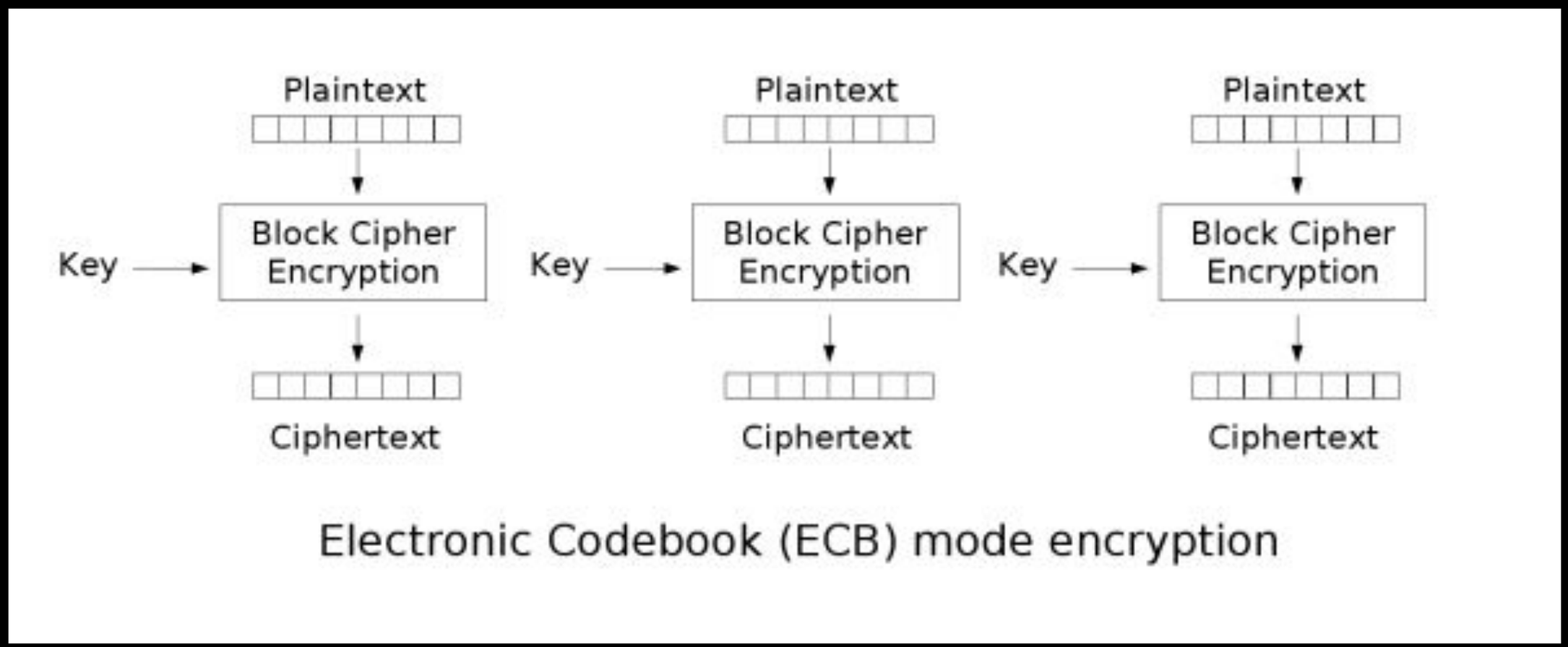
Поточные шифры

Поточные шифры - вид шифров, обрабатывающий за одну итерацию один байт (бит) путем сложения по модулю 2 с байтом (битом) гаммы.
Гамма как правило есть псевдослучайная последовательность байт, вырабатываемая генератором ключевого потока.
Текст может быть произвольной длины.
Примеры шифров: RC4, Salsa20


Генератор ключей
k_i
Источник сообщений
x_i
y_i
x_i
Приемник сообщений
Отправитель
Получатель

Блочные шифры. Режимы шифрования

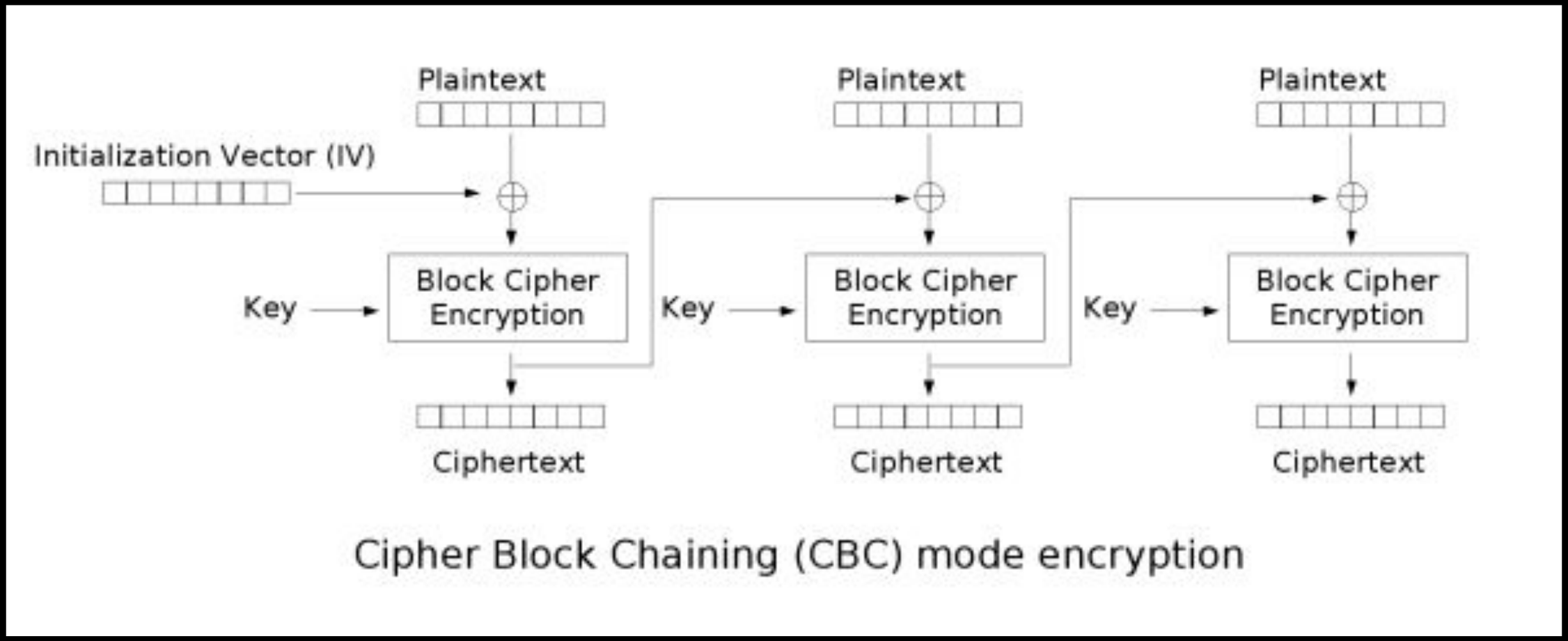
ECB



Electronic Codebook (ECB) mode encryption

Блочные шифры. Режимы шифрования

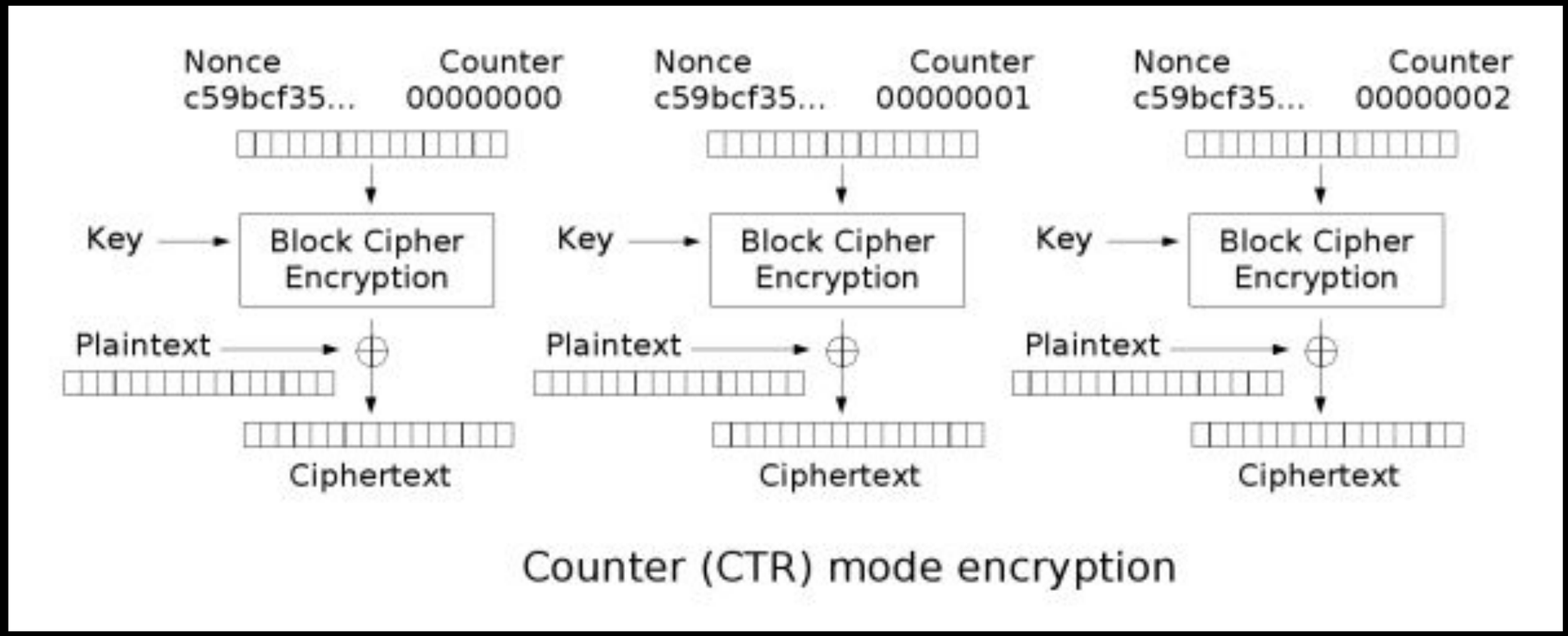
CBC



Cipher Block Chaining (CBC) mode encryption

Блочные шифры. Режимы шифрования

CTR



Counter (CTR) mode encryption

Атаки на блочные шифры

Часто встречаются в CTF:

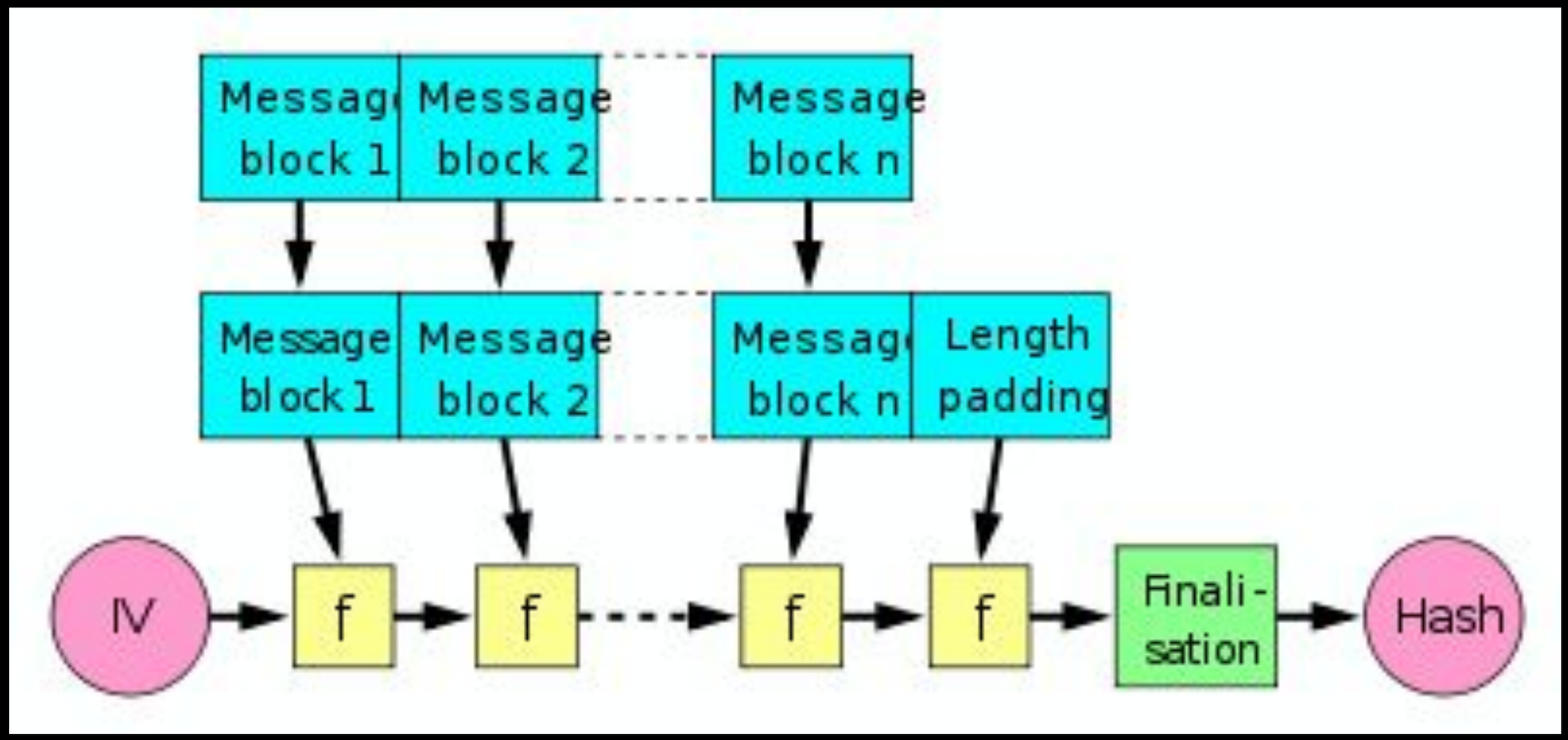
- Атаки на шифрование и расшифрование по сторонним каналам (padding oracle attack, compression attack, ...)
- Использование шифра не по назначению (например, использование шифра для обеспечения целостности зашифрованного сообщения)
- ....

Атаки на поточные шифры

Часто встречаются в CTF:

- Атаки с известным открытым текстом
- Использование шифра не по назначению (например, использование шифра для обеспечения целостности зашифрованного сообщения)
- Использование слабых генераторов ключевого потока
- ....

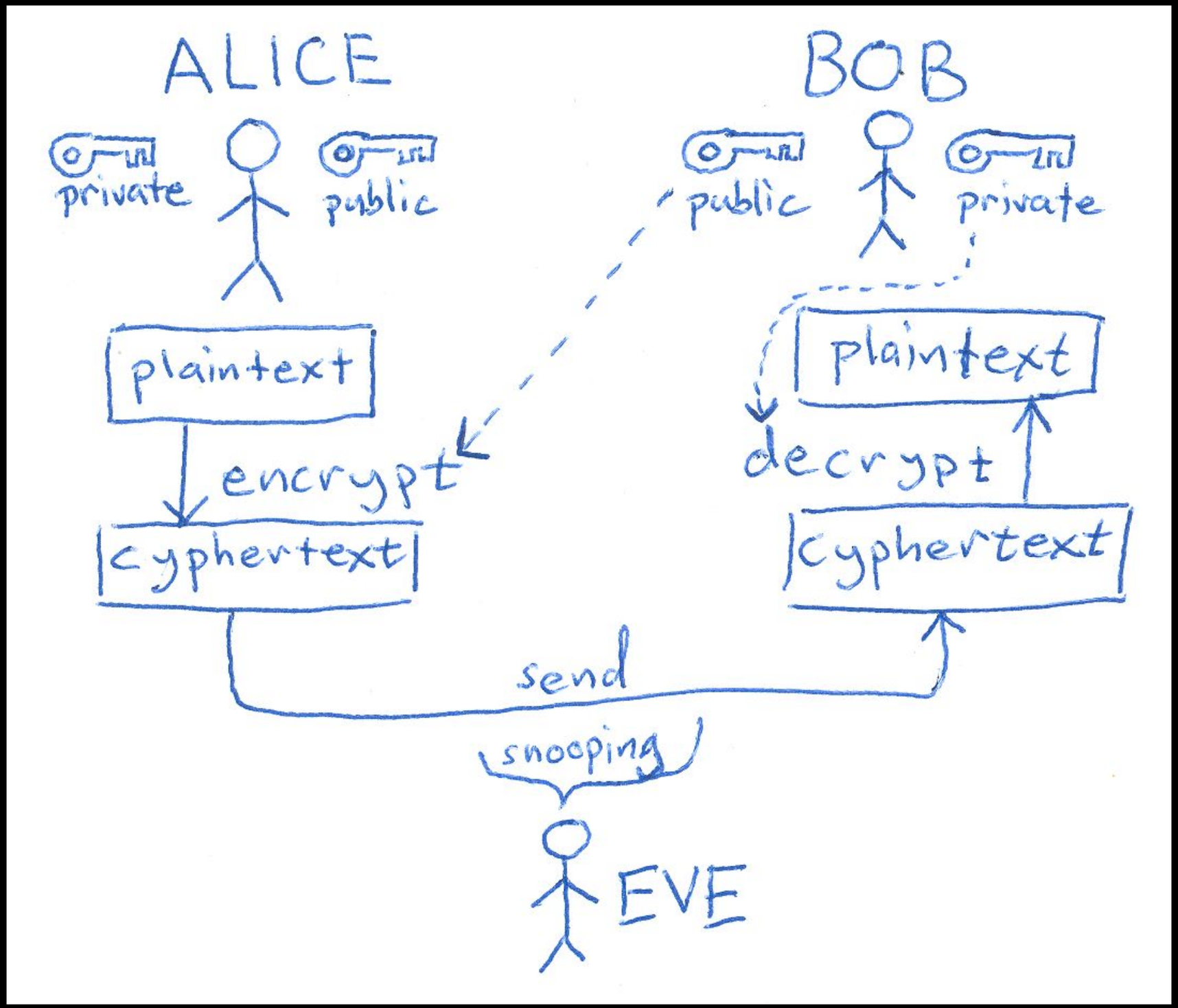
Немного о хэш-функциях



Атаки на хэш-функции

- атаки по словарю
- length-extension attack
- поиск элемента из прообраза(для хэша U такого V, что H(U) = V), поиск коллизий - годится только для криптографически нестойких функций
- ...

Немного о криптографии с открытым ключом



RSA

РАБОЧАЯ СРЕДА

- Python (или любой другой скриптовый язык)
- Sage, libnum, pycrypto, …
- Онлайн-сервисы (в интернетах, например http://www.cryptoclub.org/)
- ручка с тетрадкой :)

С ЧЕГО НАЧАТЬ?

- Анализ того, что дано
  - Описание таска и его основное содержание
  - Разобрать какие криптопримитивы используются и зачем
  - Попытаться понять, в чем состоит твоя задача
  - Если криптопримитив реализован, то сравнить реализацию со стандартом (в интернетах)

SCHOOL CTF

РАЗБОР ЗАДАНИЙ