Уроки операции Ultra

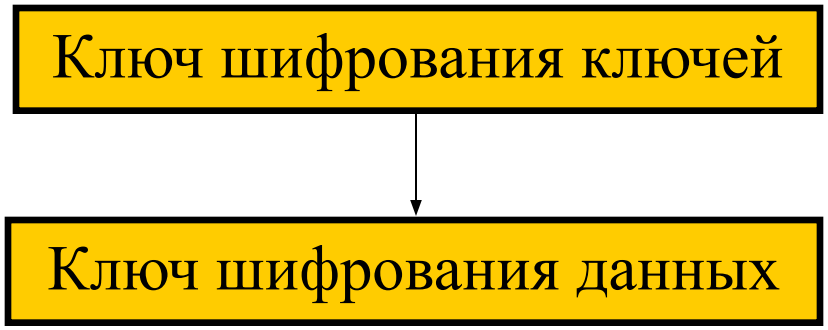
- Никогда нельзя недооценивать количество денег , времени и человеческих ресурсов, которое может мобилизовать противник .
- Перепоручение секретов машине не всегда эффективно .
- Большое количество ключей не всегда помогает .
- Атаку можно организовать всегда, если есть представление об исходном тексте.
- Нельзя позволять людям самим генерировать ключи.
- Управление ключами — слабое звено.
- Люди — самое слабое звено .

Управление ключами

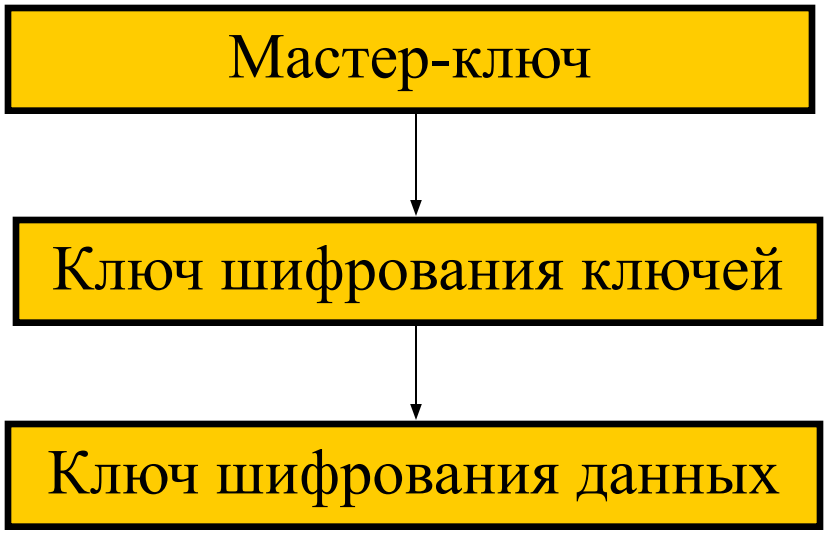
- Генерация ключей
- Распределение ключей
- Хранение ключей
- Замена ключей
- Депонирование ключей
- Уничтожение ключей

ХРАНЕНИЕ КЛЮЧЕЙ

Двухуровненевая система



Трехуровненевая система



- МК хранится в защищенном от считывания, записи и разрушающих воздействий модуле системы защиты
- МК распространяется неэлектронным способом, исключающим его компроментацию
- В системе должен существовать способ проверки аутентичности МК

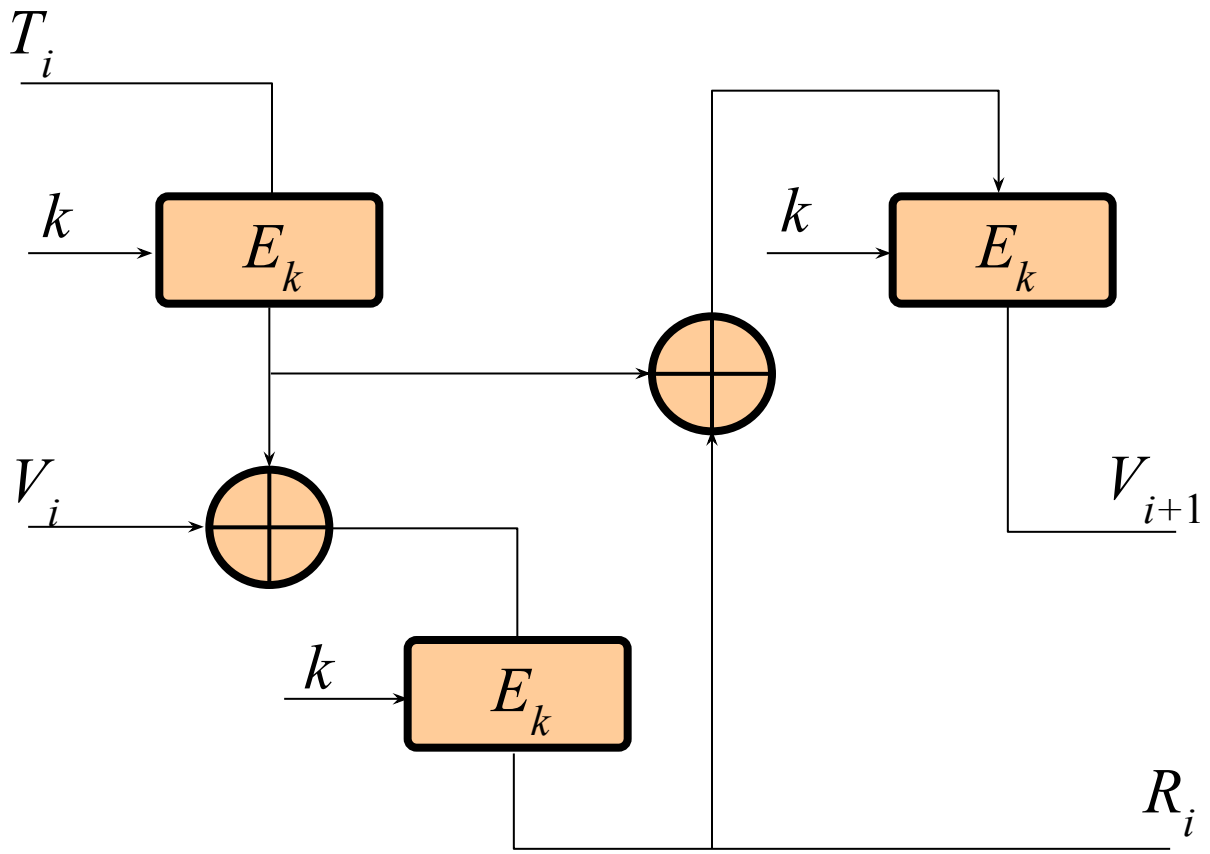
Генерация ключей

- Программная генерация - вычисление очередного псевдослучайного числа как функции текущего времени, особенности клавиатурного ввода ит.д.
- Программная генерация - основанная на моделировании генератора псевдослучайных кодов (ГПК) с равномерным законом распределения
- Аппаратная генерация - с использованием генератора псевдослучайных кодов (ГПК)
- Аппаратная генерация - с использованием генераторов случайных последовательностей, построенных на основе физических генераторов шума и качественного ГПК

Разрядность ключа

КРИПТОСИСТЕМА С СЕКРЕТНЫМ КЛЮЧОМ	КРИПТОСИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ
56	384
64	512
80	768
112	1792
128	2304

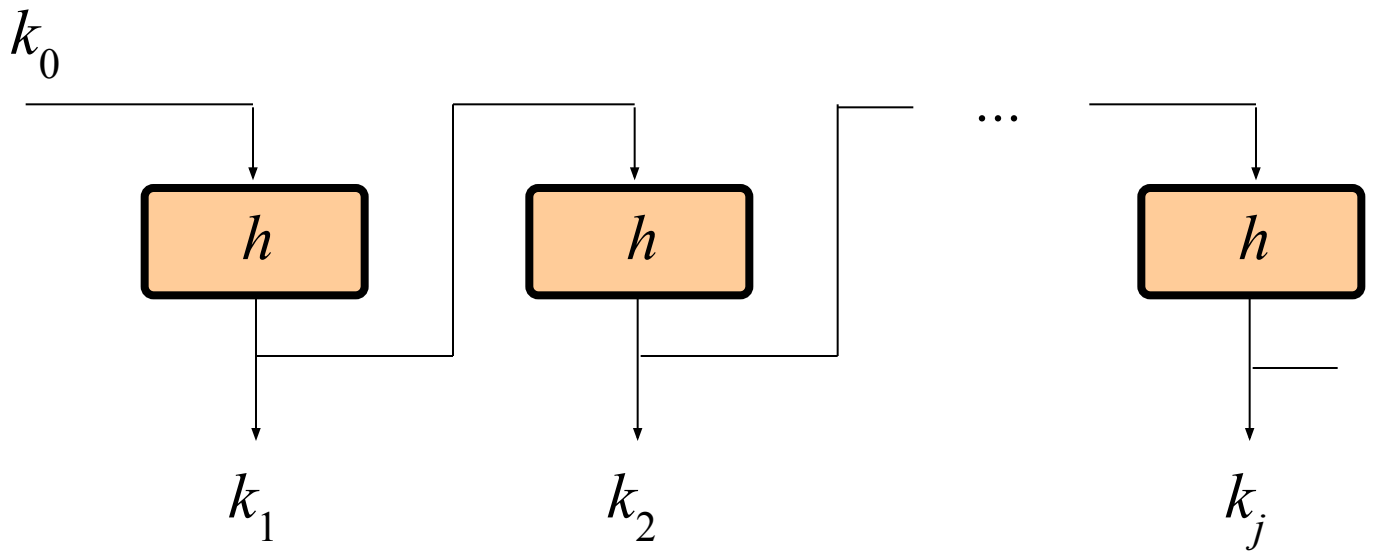
Схема генерации ключей по стандарту ANSI X9.17



T_i - временная отметка, k - МК, E_k - ф-я зашифрования DES, V_0 - секретная синхропосылка, R_i - сеансовый ключ

$$R_i = E_k(E_k(T_i) \oplus V_i) \qquad V_{i+1} = E_k(E_k(T_i) \oplus R_i)$$

Процедура модификации ключей



h - хэш-функция

Схема аутентификация МК

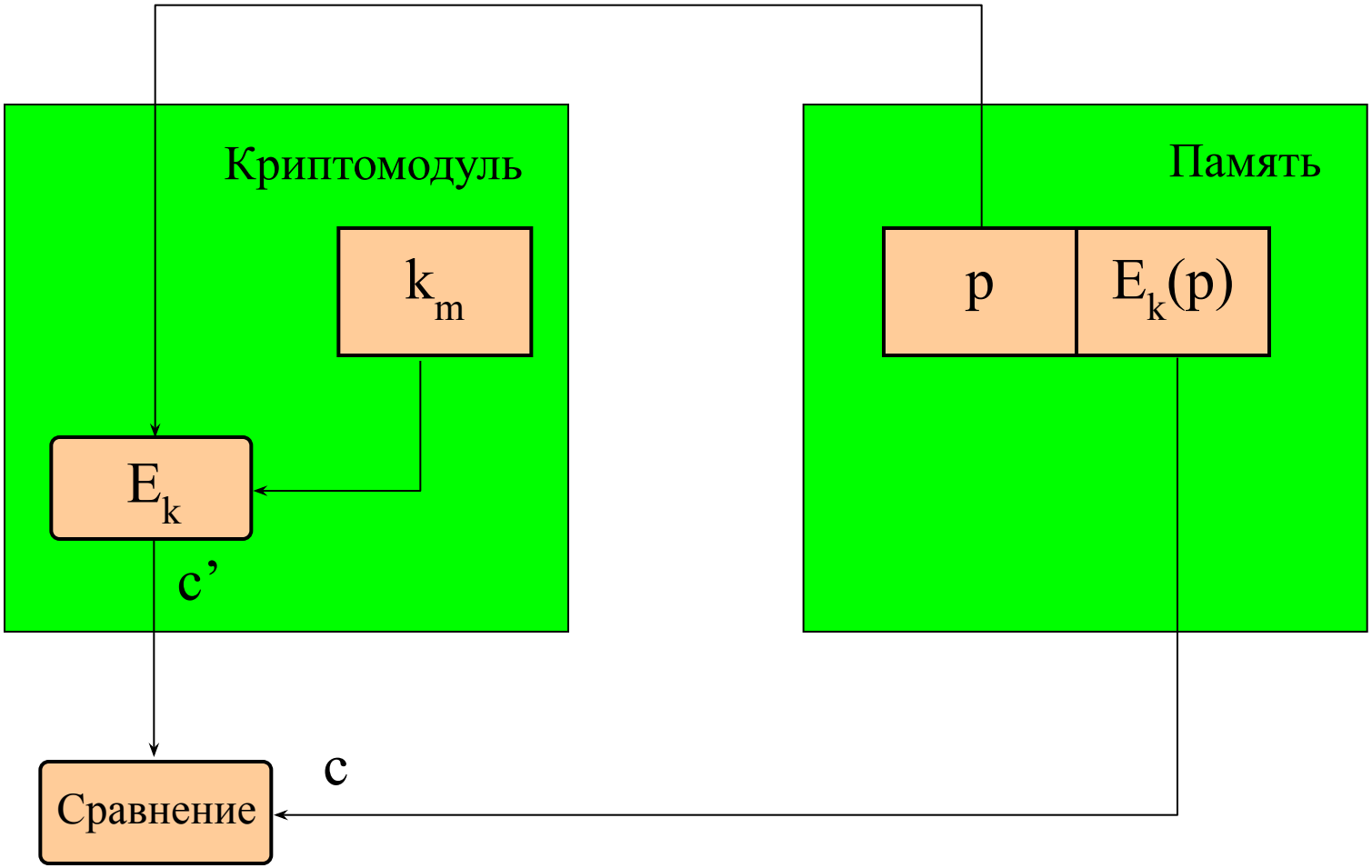
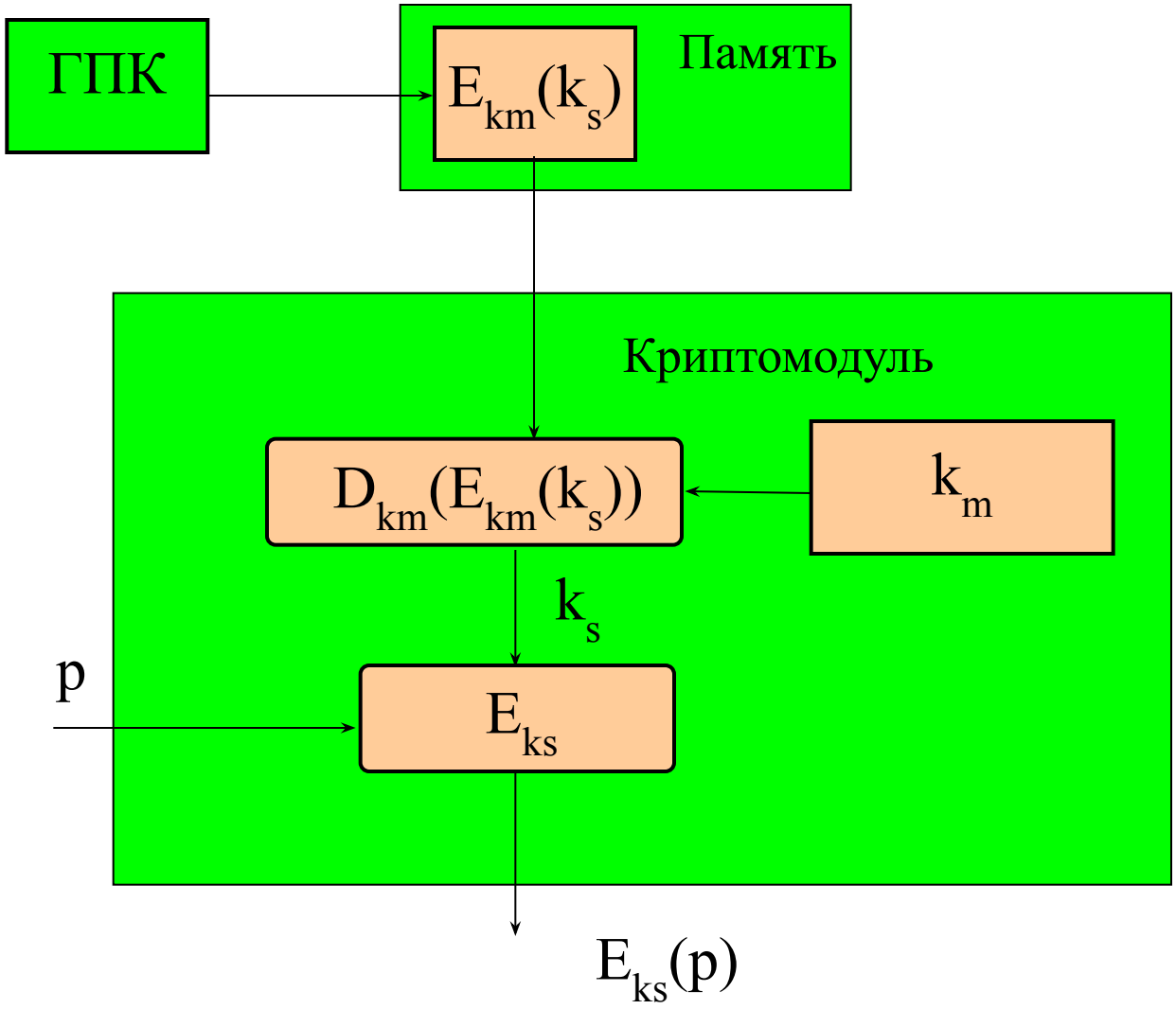
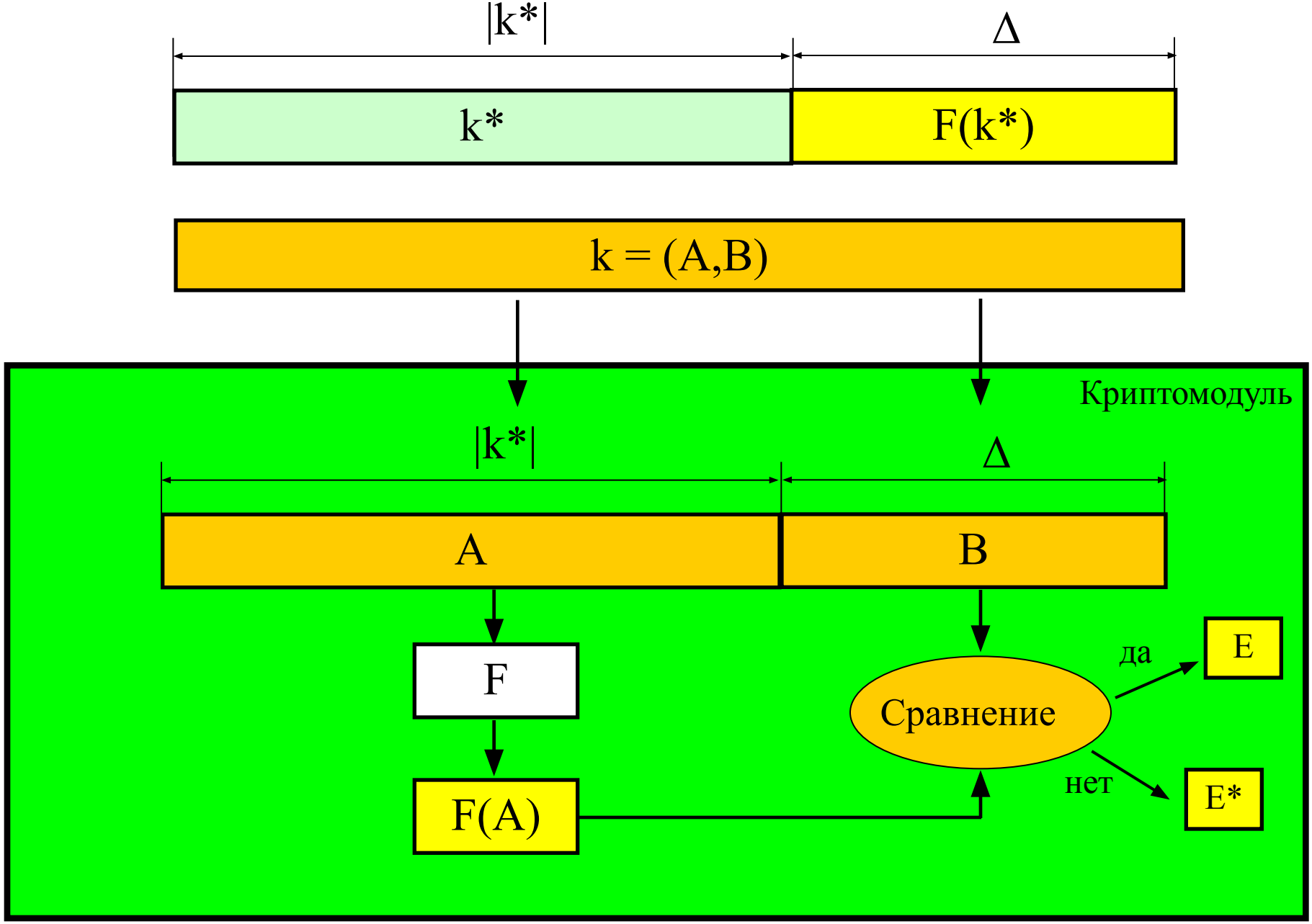


Схема защиты сеансового ключа



Неоднородное ключевое пространство



Варианты хранения ключей в криптосистеме с одним пользователем

- Запоминание пароля *pw* и в случае необходимости получение из него ключа с использованием хэш-функции: $k = h(pw)$
- Запоминание начального заполнения качественного ГПК
- Использование смарт-карты или флеш-диска

Символы ключа	**Число символов**	**Число возможных ключей (8 символов)**	**Время полного перебора (10^6кл/с)**
Заглавные буквы	32	$1{,}1 \times 10^{12}$	13 дней
Заглавные буквы и цифры	42	$9{,}7 \times 10^{12}$	112 дней
Все 8-разрядные коды	256	$1{,}9 \times 10^{19}$	600 000 лет

Время жизни ключей

Длительность времени использования зависит:

- от частоты использования ключей
- величины ущерба от компроментации ключа
- объема и характера защищаемой информации

Следует учесть, что:

- чем дольше используется ключ, тем больше вероятность его компрометации
- чем дольше используется ключ, тем больший потенциальный ущерб может нанести его компрометация
- чем больший объем информации, зашифрованной на одном ключе, перехватывает противник, тем легче производить атаку на ключ
- при длительном использовании ключа у противника появляется дополнительный стимул потратить на его вскрытие значительные ресурсы