КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ ЗАЩИТЫ ИНФОРМАЦИИ В РАДИОКАНАЛАХ СЕТЕВЫХ СПУТНИКОВЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ АСИММЕТРИЧНЫХ АЛГОРИТМОВ

Гижевская Валерия, 6413

ЦЕЛЬ:

Рассмотреть способ защиты информации на космических связях с использованием асимметричных алгоритмов

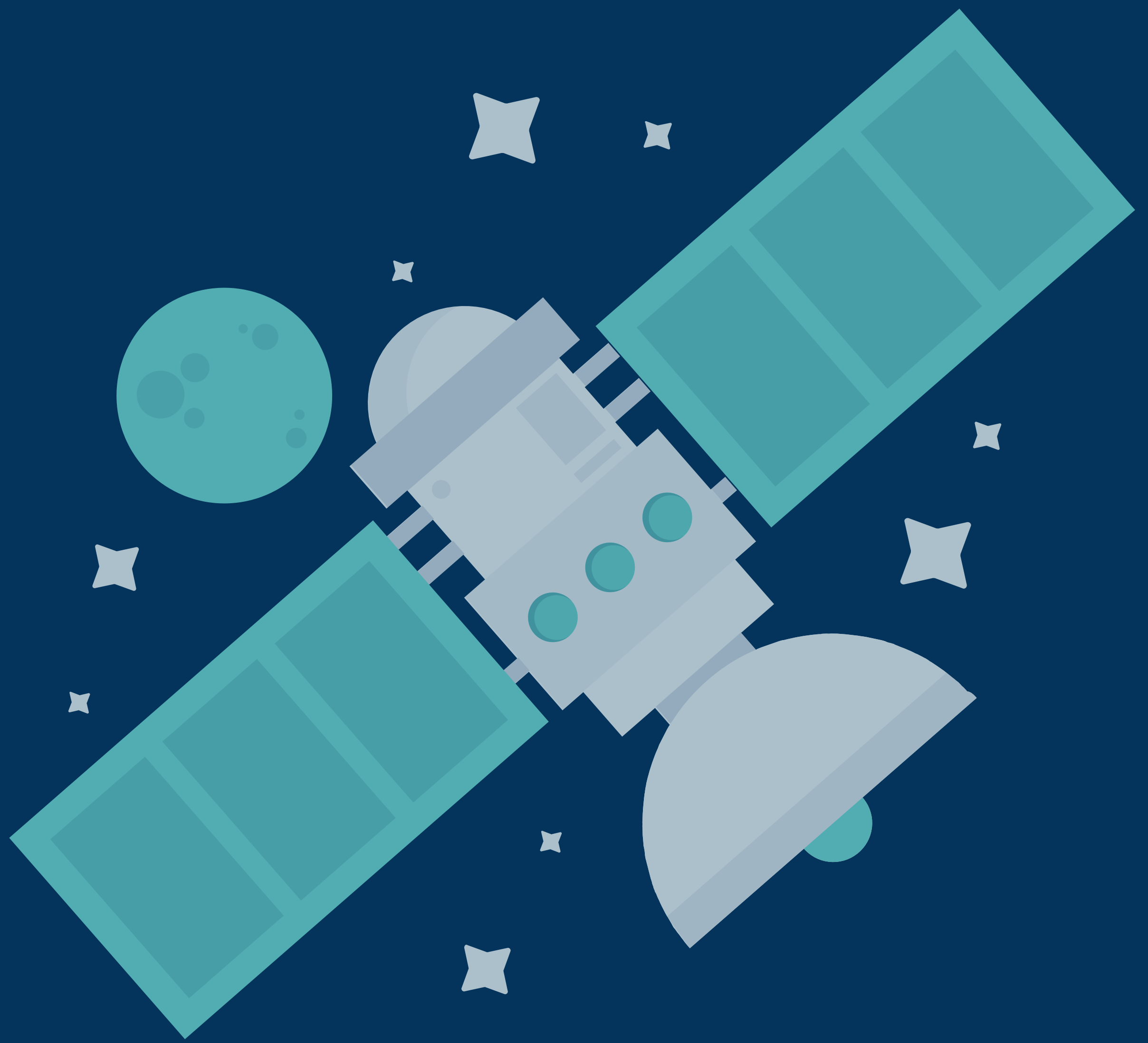
ЗАДАЧИ:

1. Рассмотреть варианты угроз безопасности информации
2. Выделить преимущества использования ассиметричных криптосистем
3. Изучить способ построения асимметричных криптоалгоритмов

Среди множества угроз безопасности информации в сетевых спутниковых системах можно выделить:

- перехват в радиоканале (контроль трафика)
- воздействие преднамеренных помех;
- несанкционированное декодирование и дешифрование информации
- информационную перегрузку за счёт передачи большого количества фрагментов ложной информации
- передачу ложной информации (в том числе ложной командно-программной информации), постановку имитирующих помех;
- физическое воздействие на оконечные устройства

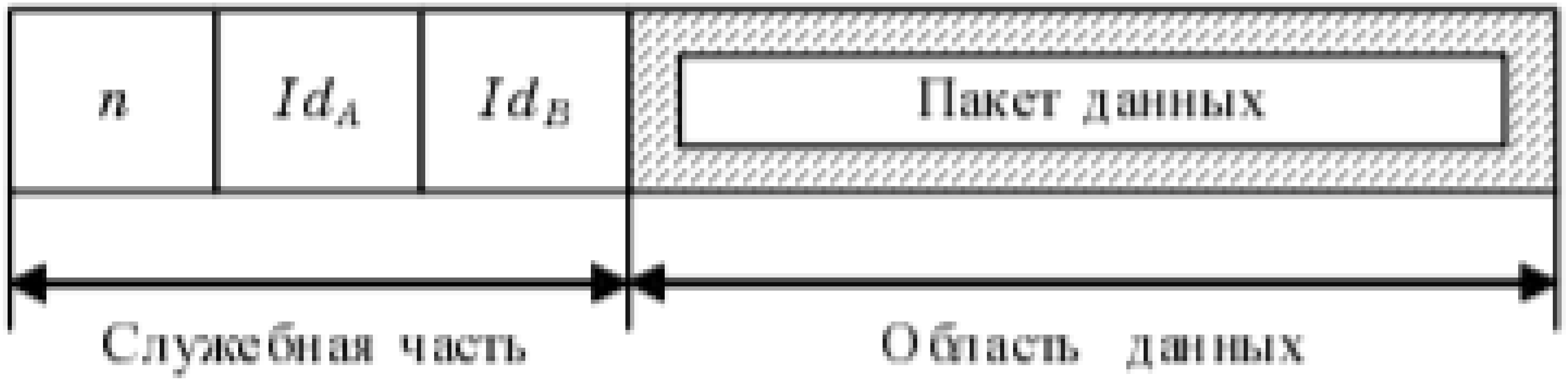
Преимущества



В сетях с большим количеством абонентов часто возникают ситуации, когда абоненты не могут доверять друг другу, а асимметричные криптосистемы позволяют строить эффективные алгоритмы аутентификации

Использование для защиты информации в сетях с большим количеством абонентов только симметричных криптосистем требует распространения большого числа ключевой информации, а асимметричные криптосистемы свободны от данного недостатка

В данном случае пакет будет состоять из служебной части и области данных (рис. 1). В служебной части передаются номер пакета (n), адреса абонентов (идентификаторы IdA и IdB), другая служебная информация (например, флаги). В области данных передаётся зашифрованный пакет информационного обмена абонентов. В случае, если длина зашифрованного пакета превышает размер области данных пакета используемой сети связи, последний может быть разбит на несколько частей в соответствии с принятыми стандартами.



■ *Рис. 1. Структура пакета*

Рассмотрим математические основы использования эллиптических кривых в криптографических целях. Рассмотрим эллиптическую группу по модулю p, где p является простым числом. Выберем два неотрицательных целых числа a и b, меньшие p и удовлетворяющие условию

$$4a^3 + 27b^2 (mod\ p) \neq 0$$

Эллиптическую кривую (ЭК) над конечным полем Галуа GFp можно представить в виде

$$E_p(a, b)\colon y^2 = x^3 + ax + b\ (mod\ p)$$

Операция обращения точки для кривой записывается следующим образом:

$$-(x, y) = (x, -y).$$

Групповой закон сложения точек $P_1 \oplus P_2$ имеет вид $P_1 \oplus P_2 = (x_3, y_3)$, где

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_2 - x_1$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

При $P_1 = P_2 = (x_1, y_1)$, получаем $2P_1 = (x_2, y_2)$:

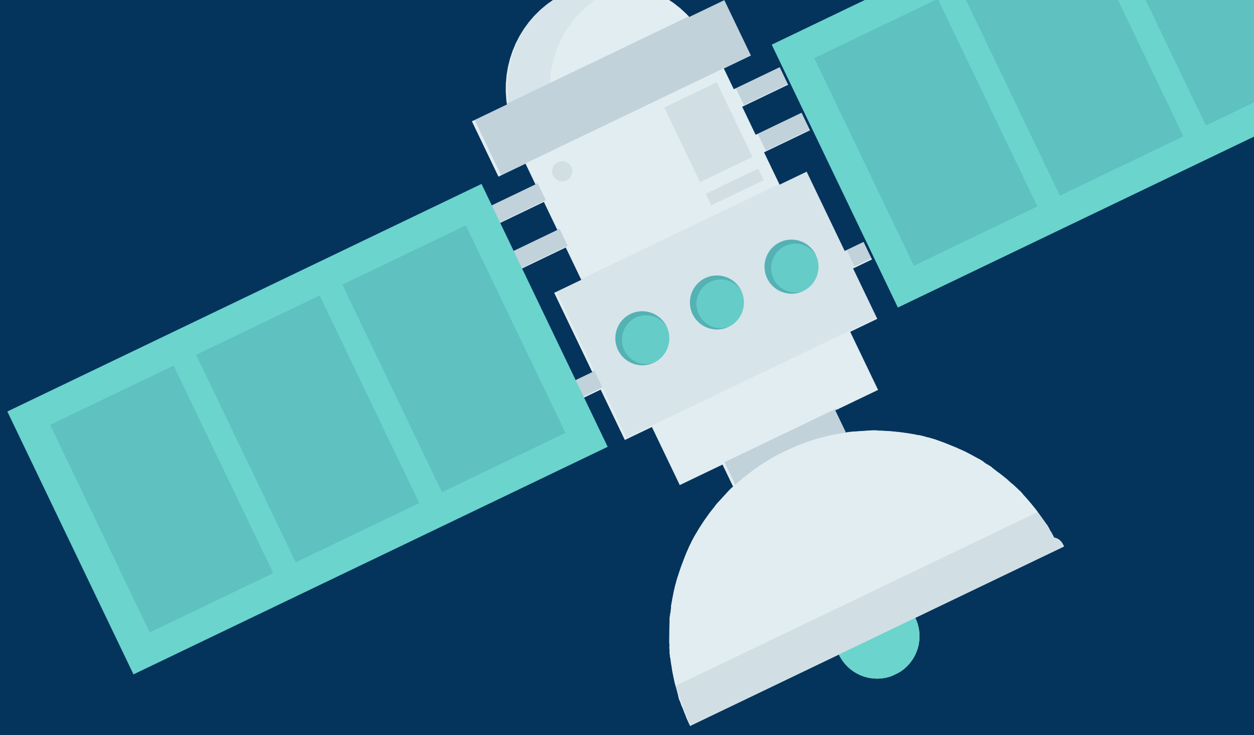
$$x_2 = \frac{(3x_1^2 + a)^2}{4y_1^2} - 2x_1$$

$$y_2 = \frac{(3x_1^2 + a)}{2y_1}(x_1 - x_2) - y_1$$

Пусть p – простое число, а G – примитивный элемент или генератор аддитивной циклической подгруппы группы точек ЭК; P – произвольная точка, принадлежащая данной кривой. Тогда любую точку P кривой E(GFp) можно представить как кратную генератору подгруппы в виде

$$P = n \times G = \underbrace{G \oplus G \oplus \ldots \oplus G}_{n\ \text{раз}},$$

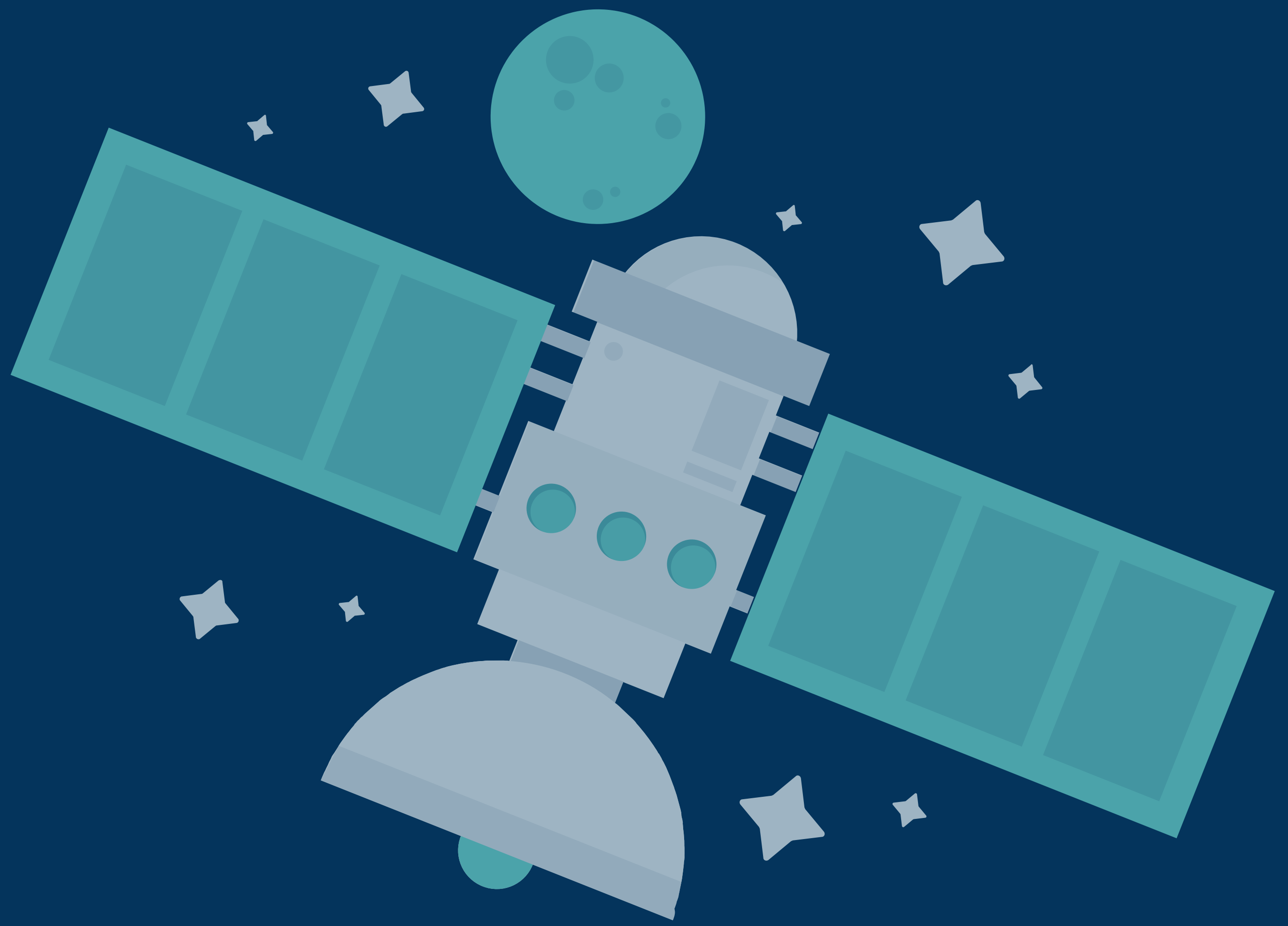
Групповой закон сложения точек аддитивной абелевой группы ЭК обладает следующим криптографическим свойством: нахождение числа n по двум заданным элементам группы P и G при $n \to \infty$ является вычислительно сложной задачей. Таким образом, групповой закон сложения точек ЭК рассматривается в качестве функции криптографического преобразования.



ВЫВОДЫ:

- Рассмотрели варианты угроз безопасности информации
- Выделили преимущества использования ассиметричных криптосистем
- Изучили способ построения асимметричных криптоалгоритмов

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ



ЗАЩИТА ИНФОРМАЦИИ

А. А. Корниенко
доктор техн. наук, профессор
Санкт-Петербургский государственный университет путей сообщения
С. В. Штанько
канд. техн. наук
Военно-космическая академия им. А. Ф. Можайского

Спасибо за внимание