

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»  
(СПбГУТ)

---

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

**Лабораторная работа №3**

Анализ системы шифрования по ее графовой модели

Выполнил студент группы ИКТЗ-83:

Громов А.А. Вариант: 4

(Ф.И.О., № группы)

\_\_\_\_\_  
(подпись)

Проверил:

Яковлев В.А.

(уч. степень, уч. звание, Ф.И.О.)

\_\_\_\_\_  
(подпись)

Санкт-Петербург

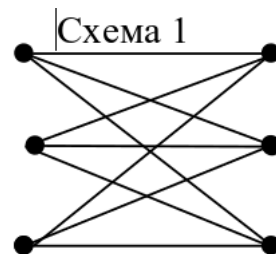
2021

**Цель лабораторной работы:** Научиться оценивать стойкость системы шифрования по графовой модели.

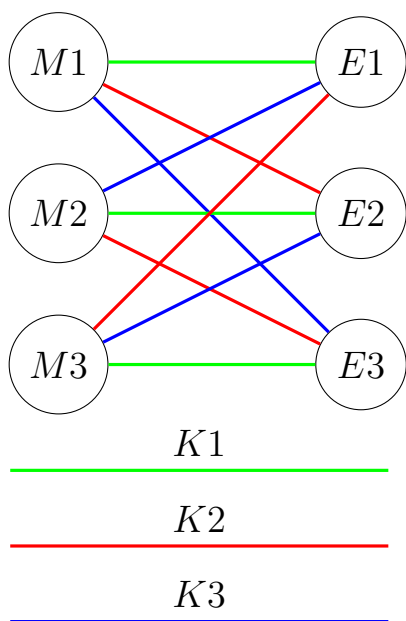
### Исходные данные

Априорные вероятности сообщений			Вероятности ключей		
P(M1)	P(M2)	P(M3)	P(K1)	P(K2)	P(K3)
0.4	0.5	0.1	равновероятны		

Граф системы шифрования



### Расчеты



Расчет сумм вероятностей ключей:

$$P(E_1|M_1) = \sum_s P(K)_s = \frac{1}{3}$$

$$P(E_1|M_2) = \sum_s P(K)_s = \frac{1}{3}$$

$$P(E_1|M_3) = \sum_s P(K)_s = \frac{1}{3}$$

$$P(E_2|M_1) = \sum_s P(K)_s = \frac{1}{3}$$

$$P(E_2|M_2) = \sum_s P(K)_s = \frac{1}{3}$$

$$P(E_2|M_3) = \sum_s P(K)_s = \frac{1}{3}$$

$$P(E_3|M_1) = \sum_s P(K)_s = \frac{1}{3}$$

$$P(E_3|M_2) = \sum_s P(K)_s = \frac{1}{3}$$

$$P(E_3|M_3) = \sum_s P(K)_s = \frac{1}{3}$$

Расчет вероятностей криптограмм:

$$P(E_1) = \sum_{i=1}^{m^n} P(M_1)P(E_1|M_1) = 0.4 \cdot \frac{1}{3}$$

$$P(E_1) = \sum_{i=1}^{m^n} P(M_2)P(E_1|M_2) = 0.5 \cdot \frac{1}{3}$$

$$P(E_1) = \sum_{i=1}^{m^n} P(M_3)P(E_1|M_3) = 0.1 \cdot \frac{1}{3}$$

$$P(E_2) = \sum_{i=1}^{m^n} P(M_1)P(E_2|M_1) = 0.4 \cdot \frac{1}{3}$$

$$P(E_2) = \sum_{i=1}^{m^n} P(M_2)P(E_2|M_2) = 0.5 \cdot \frac{1}{3}$$

$$P(E_2) = \sum_{i=1}^{m^n} P(M_3)P(E_2|M_3) = 0.1 \cdot \frac{1}{3}$$

$$P(E_3) = \sum_{i=1}^{m^n} P(M_1)P(E_3|M_1) = 0.4 \cdot \frac{1}{3}$$

$$P(E_3) = \sum_{i=1}^{m^n} P(M_2)P(E_3|M_2) = 0.5 \cdot \frac{1}{3}$$

$$P(E_3) = \sum_{i=1}^{m^n} P(M_3)P(E_3|M_3) = 0.1 \cdot \frac{1}{3}$$

$$P(E_1) = P(M_1)P(E_1|M_1) + P(M_2)P(E_1|M_2) + P(M_3)P(E_1|M_3) = 0.4 \cdot \frac{1}{3} + 0.5 \cdot \frac{1}{3} + 0.1 \cdot \frac{1}{3} = \frac{1}{3}$$

$$P(E_2) = P(M_1)P(E_2|M_1) + P(M_2)P(E_2|M_2) + P(M_3)P(E_2|M_3) = 0.4 \cdot \frac{1}{3} + 0.5 \cdot \frac{1}{3} + 0.1 \cdot \frac{1}{3} = \frac{1}{3}$$

$$P(E_3) = P(M_1)P(E_3|M_1) + P(M_2)P(E_3|M_2) + P(M_3)P(E_3|M_3) = 0.4 \cdot \frac{1}{3} + 0.5 \cdot \frac{1}{3} + 0.1 \cdot \frac{1}{3} = \frac{1}{3}$$

#### Расчет апостериорных вероятностей всех сообщений:

$$P(M_1|E_1) = \frac{P(E_1|M_1)P(M_1)}{P(E_1)} = \frac{\frac{1}{3} \cdot 0.4}{\frac{1}{3}} = 0.4$$

$$P(M_1|E_2) = \frac{P(E_2|M_1)P(M_1)}{P(E_2)} = \frac{\frac{1}{3} \cdot 0.4}{\frac{1}{3}} = 0.4$$

$$P(M_1|E_3) = \frac{P(E_3|M_1)P(M_1)}{P(E_3)} = \frac{\frac{1}{3} \cdot 0.4}{\frac{1}{3}} = 0.4$$

$$P(M_2|E_1) = \frac{P(E_1|M_2)P(M_2)}{P(E_1)} = \frac{\frac{1}{3} \cdot 0.5}{\frac{1}{3}} = 0.5$$

$$P(M_2|E_2) = \frac{P(E_2|M_2)P(M_2)}{P(E_2)} = \frac{\frac{1}{3} \cdot 0.5}{\frac{1}{3}} = 0.5$$

$$P(M_2|E_3) = \frac{P(E_3|M_2)P(M_2)}{P(E_3)} = \frac{\frac{1}{3} \cdot 0.5}{\frac{1}{3}} = 0.5$$

$$P(M_3|E_1) = \frac{P(E_1|M_3)P(M_3)}{P(E_1)} = \frac{\frac{1}{3} \cdot 0.1}{\frac{1}{3}} = 0.1$$

$$P(M_3|E_2) = \frac{P(E_2|M_3)P(M_3)}{P(E_2)} = \frac{\frac{1}{3} \cdot 0.1}{\frac{1}{3}} = 0.1$$

$$P(M_3|E_3) = \frac{P(E_3|M_3)P(M_3)}{P(E_3)} = \frac{\frac{1}{3} \cdot 0.1}{\frac{1}{3}} = 0.1$$

#### **Выводы**

Т.к.  $P(M_1|E_j) = P(M_1)$ ,  $P(M_2|E_j) = P(M_2)$ ,  $P(M_3|E_j) = P(M_3)$ , то система шифрования является безусловно стойкой из условия АССШ  $P(M|E) = P(M)$ .