

число людей, которые могут заболеть в некоторый момент времени  $t$ . Тогда имеем  $X(t) + Y(t) = N + 1$  в любой момент времени. Количество новых больных  $dX$  появившихся за промежуток времени  $dt$  будет пропорционально числу встреч здоровых и заболевших людей.

Следовательно,  $dX = aXYdt = aX(N + 1 - X)dt$  при  $X(0) = 1$ . Найдем общее решение, предварительно разделив переменные, имеем

$$\frac{dx}{X(N + 1 - X)} = a dt,$$

после интегрирования выразим искомую функцию

$$X(t) = \frac{N + 1}{Ce^{-at(N+1)} + 1}.$$

Учитывая начальные условия, имеем  $C = N$  найдем число заболевших как функцию времени:

$$X(t) = \frac{N + 1}{Ne^{-at(N+1)} + 1}.$$

Проанализируем результат, при возрастании  $t$ ,  $X(t)$  – увеличивается, что согласуется с общепринятыми представлениями.

УДК 004.056.55

Студ. Е.И. Чабоха, М.В. Воронова  
 Науч. рук. зав. кафедрой О.Н. Пыжкова  
 (Кафедра высшей математике БГТУ)

### ТАЙНЫ ЗА СЕМЬЮ ПЕЧАТЯМИ

Греческий термин «криптография» означает «секретный шрифт», как доказали ученые, тексты начали шифровать уже в третьем тысячелетии до нашей эры. Как в Римской империи, так и в Средневековье, важные сообщения и военные приказы зашифровывались с помощью основных способов шифрования информации: метода перестановок (метод одиночной перестановки по ключу) и метода подстановки (шифровальные диски).

*Шифр Виженера.* Эта система была придумана французским дипломатом Блезом Виженером. Преимущество данного метода заключается в том, что каждую букву можно закодировать 33 различными способами – в основе алгоритма лежит таблица, включающая в себе

33 строки с алфавитном, и каждая строка начинается со следующей буквы. Шифр Виженера – это последовательность шифров Цезаря с различными значениями сдвига. Если номер алфавита заменяется в каждом сообщении, шансы разгадать шифр по частотному коду значительно падают. Но расшифровка становится еще более сложной. Например, попробуем зашифровать «Мама мыла раму» с ключом «кошка» в результате получим «чоек мёш ыачв». В современных условиях никто не шифрует вручную, для этого используют, например, программу **Cryptools** или пишут код на **Python**.

Военным пришлось развивать криптографические системы и выводить их на самый современный уровень, особенно во время Второй мировой войны. Криптоанализ привлек все возможные математические и статистические ресурсы для дешифровки сообщений врага.

Один из способов усложнить дешифровку сообщения – это использование языка, не имеющего письменности: язык индейцев навахо. Эта идея принадлежала Филиппу Джонстону, который говорил на языке навахо, так как вырос в резервации. Навахо очень сложный язык, его звучание представляет собой странное чередование назальных гортанных звуков, которые почти невозможно записать. Отсутствие в языке навахо военных терминов компенсировали, другими словами. например, истребители называли «колибри», разведчики «филины», «бомбы» – «яйца». Благодаря индейцам навахо армия США на атлантическом фронте имела совершенную систему связи: быструю и не поддающуюся ни дешифровке, ни фальсификации.

Криптография присутствует во многих аспектах повседневной жизни, хотя не всегда ее можно заметить невооруженным глазом.

УДК 51-78

Студ. Н.Д. Тумаш, А.П. Антошкина  
Науч. рук. доц. Л.Д. Яроцкая  
(Кафедра высшей математике БГТУ)

### **ЛОГАРИФМИЧЕСКАЯ СПИРАЛЬ В ИСКУССТВЕ**

Математика играет важную роль в изобразительном искусстве, в частности, при использовании перспективы и поиске идеальных пропорций. Художники применяют проективную геометрию, чтобы изображать реалистичные трехмерные сцены на плоском холсте или листе бумаги, создавать композиции геометрических форм в гармонии