Краснодарское высшее военное училище имени генерала армии С. М. Штеменко

11 кафедра
«Криптографических методов защиты информации»

«Китайская теорема об остатках »

Подготовил прапорщик 223 учебной группы
Кузнецов Я.Р.

Краснодар 2018 г.

Вступление

Несколько связанных утверждений известны под именем китайской теоремы об остатках. Эта теорема в её арифметической формулировке была описана в трактате китайского математика Сунь Цзы «Сунь Цзы Суань Цзин», предположительно датируемом третьим веком н.э..

Формулировка: Китайской теоремы об остатках

Любое неотрицательное целое натуральное число, не превосходящее произведения модулей, можно однозначно восстановить, если известны его вычеты по этому модулю.

Пусть числа m1, m2,…,mn попарно взаимно простые тогда система уравнений

Имеет единственное решение x=x0(mod M) , где M = m1*m2*…*mn , $x_0 = \sum_{i=1}^{n} M_i y_i C_i$, $M_i = \frac{M}{m_i}$, $M_i y_i \equiv 1 (mod\, m_i), i = \overline{1,n}$

Применение китайской теоремы об остатках

- Китайская теорема об остатках широко применяется в теории чисел, криптографии и других дисциплинах.
- Взаимно однозначное соответствие между некоторым числом и набором его остатков, определяемым набором взаимно простых чисел, существование которого утверждается в теореме, на практике помогает работать не с длинными числами, а с наборами их коротких по длине остатков. Кроме того, вычисления по каждому из модулей можно выполнять параллельно. Если в качестве базиса взять, к примеру, первые 500 простых чисел, длина каждого из которых не превосходит 12 битов, то этого хватит для представления чисел длиной до 1519 десятичных знаков (сумма десятичных логарифмов первых 500 простых чисел равна 1519,746…).

Спасибо за внимание!