криптография: от спецотдела к науке

alexander.shen@lirmm.fr, www.lirmm.fr/~ashen

LIRMM CNRS & University of Montpellier

18.08.2020

A

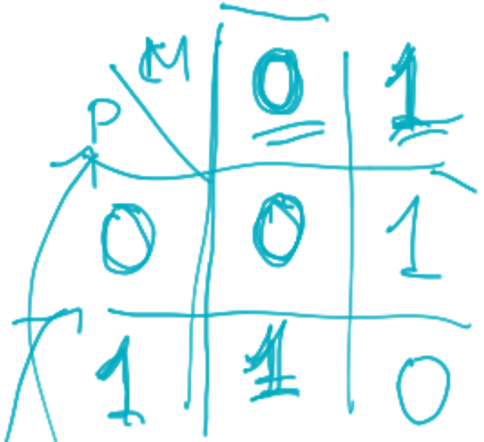
разделение: алгоритмы + ключи

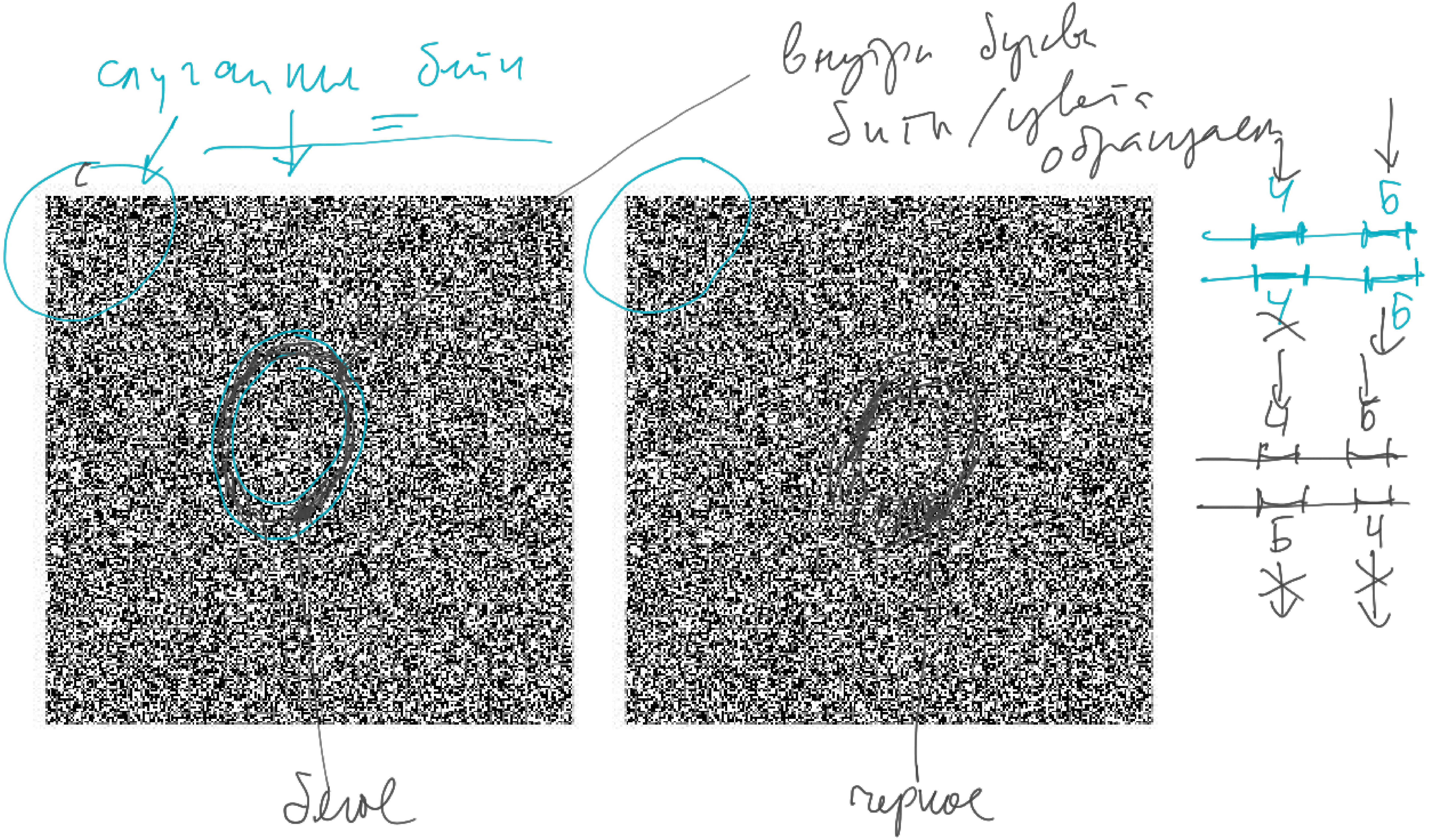
one-time pad: пример

0 4 8 2 ... ← message

→ 1 7 3 4 ... ← one time pad

анализ: xor ← 1 1 1 6 ← encoded message




случайные биты
внутри буквы
биты/цвета обращаем
Ч
Б
белое
черное

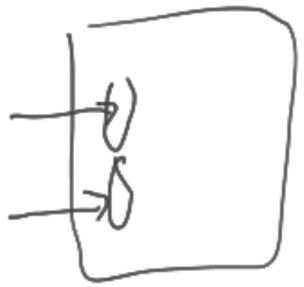
разделение секрета:

на двоих

на троих

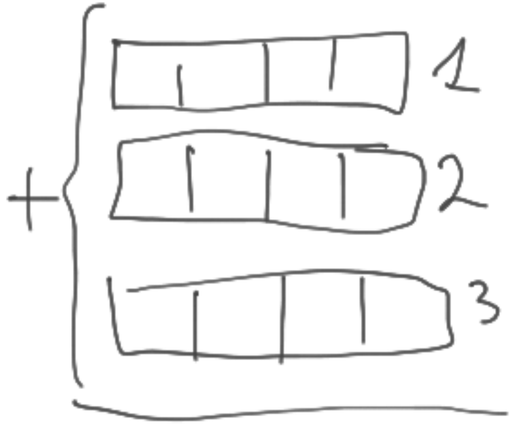
2 из 3

k из *n*



10000 → 100

0814 ← 1 страница
+ 7099 ← 2 дают
2 чего не хватает 1-му для сек. кода



код

код

x_1 x_k

$$\begin{cases} 3x_1 + 7x_2 \ldots + 17x_k \to 1 \\ 2x_1 - 3x_2 \ldots \to 2 \\ \ldots \\ \ldots \to n \end{cases}$$

A. Shamir

k неизвестн

↓

k уравнений

а) Секрет

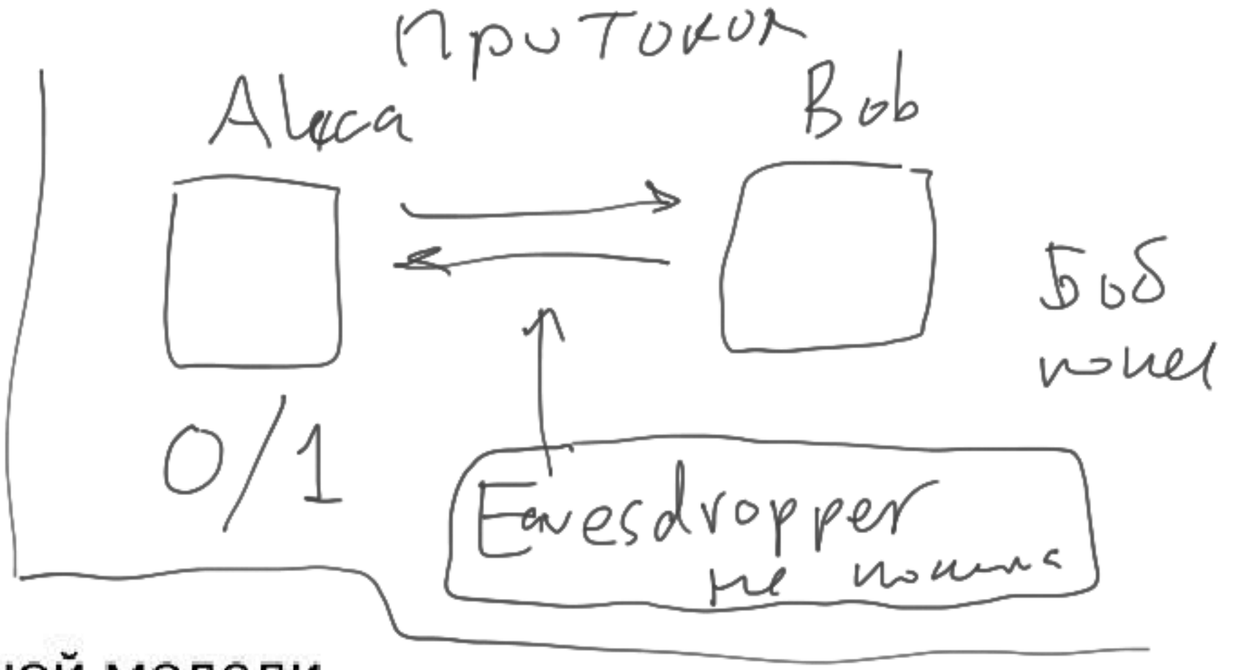
б) секретные цифры (числа)

~1980

public key cryptography

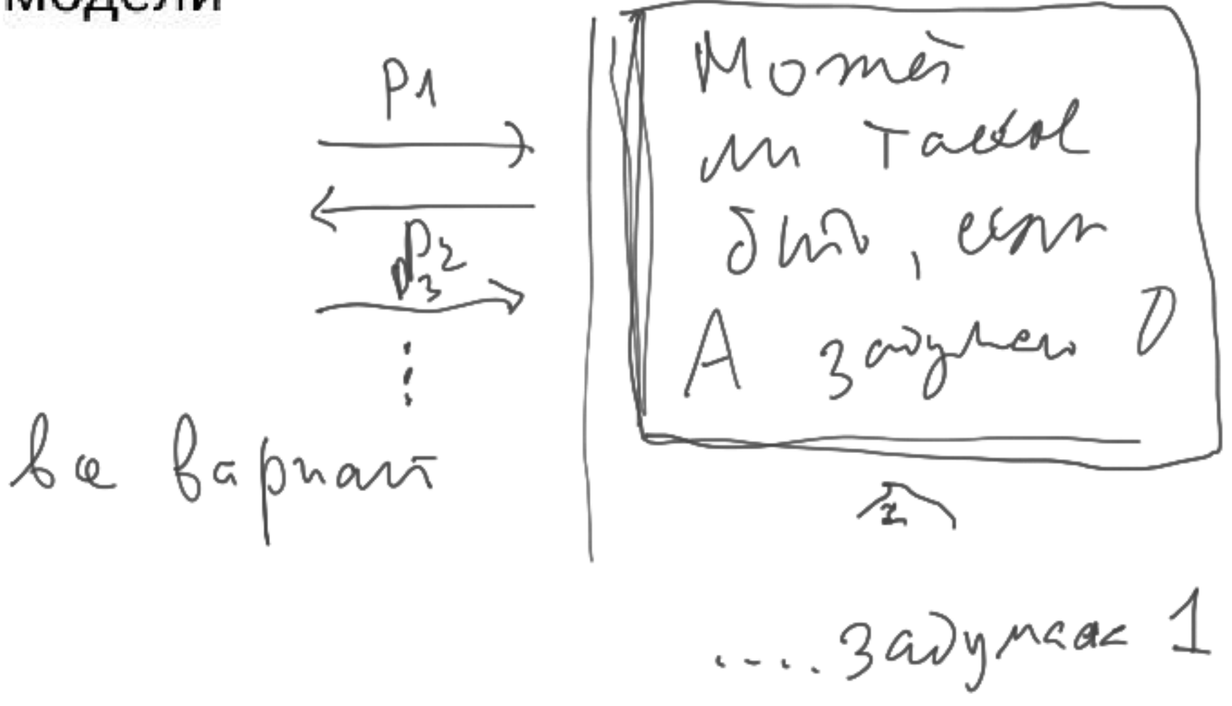
задача

неразрешимость в информационной модели



может
не может
— немедленно

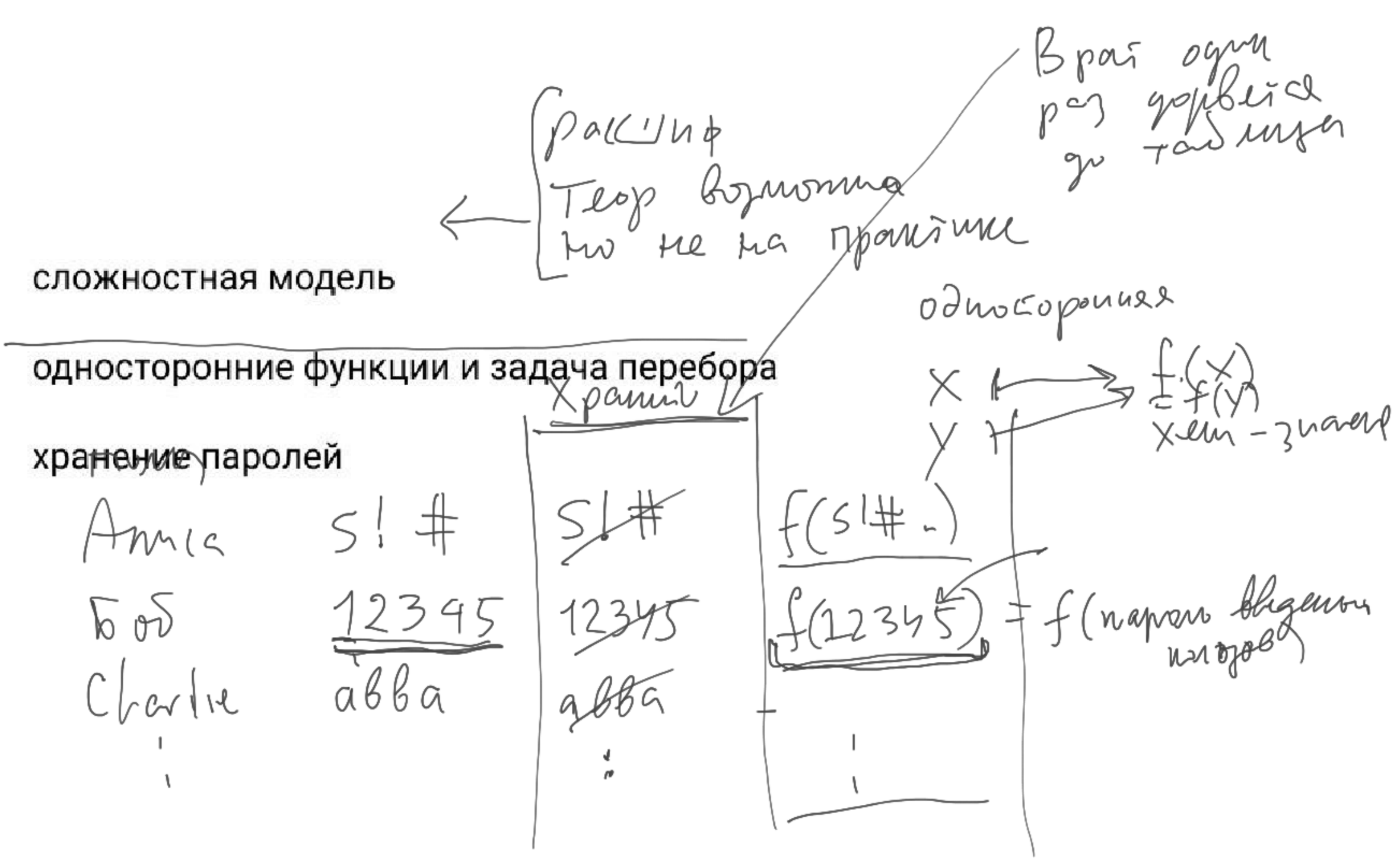
может
не может
— E : 0
1



сложностная модель

односторонние функции и задача перебора

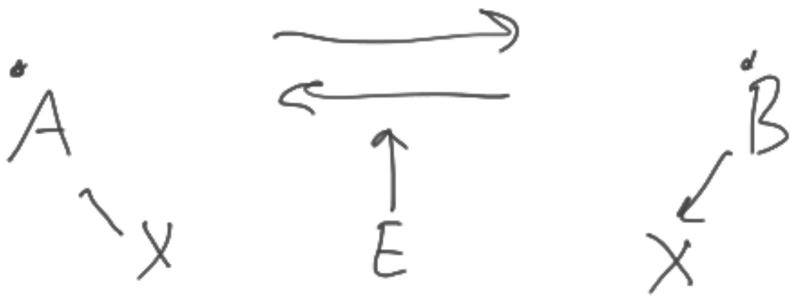
хранение паролей



Diffie–Hellman

RSA

орлянка по телефону



разложение на множители и digital cash