

MOSCOW FORENSICS DAY '25

ВЯЧЕСЛАВ ЧИКИН

«ОСОБЕННОСТИ УСКОРЕНИЯ ПЕРЕБОРА
ПАРОЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ»

ACELAB



ИСХОДНАЯ ЗАДАЧА

Подобрать пароль
из 8-ми символов



Введите пароль

Вы не вводили пароль более 72 часов. Введите пароль.

Введите пароль



ВОЗМОЖНЫЕ СИМВОЛЫ

- ▶ 1 - 9 (10)
- ▶ a - z (26)
- ▶ A - Z (26)
- ▶ Пробел ! «» # \$ % & ' () * + , - . /
: ; < = > ? @ [\] ^ _ ` { | } ~ (33)

ИТОГО: 95 возможных символов

ОСОБЕННОСТИ КЛАВИАТУРЫ

▶ ` → "`

▶ ` → z

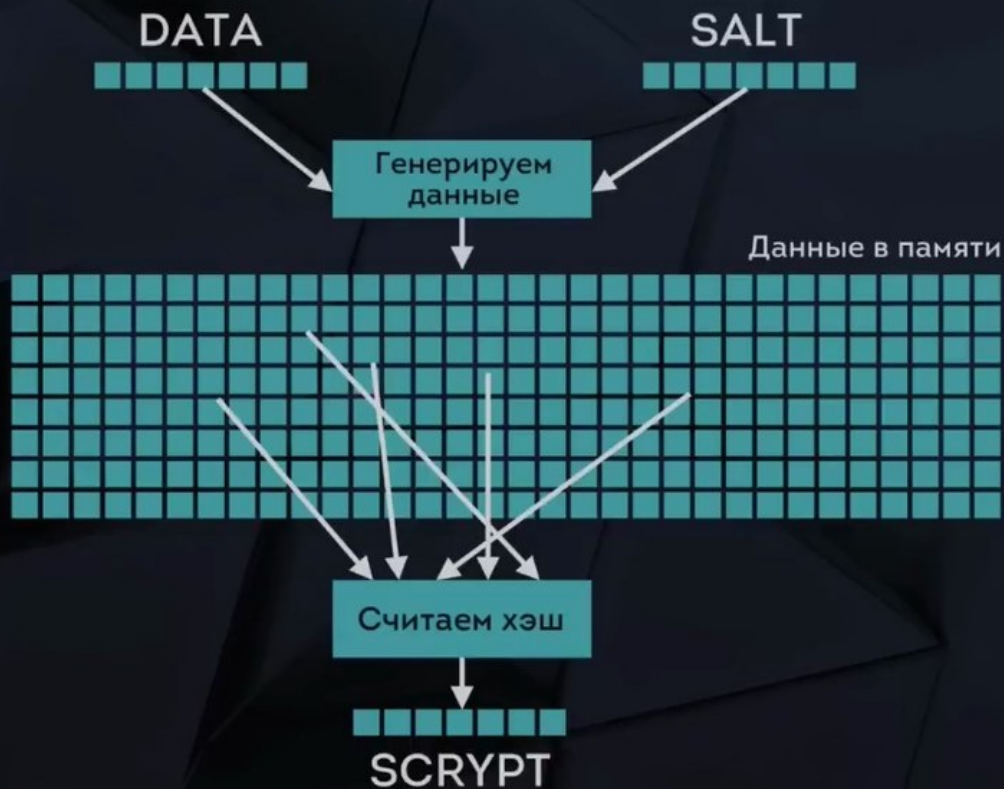
▶ ♥ → e

РАСПРОСТРАНЁННЫЕ АЛГОРИТМЫ



- ▶ SHA256
- ▶ SCRIPT

РАБОТА SCRIPT



1. **N** (cost factor) – Фактор стоимости (CPU/Память)

- ▶ **Что это?** Главный параметр, определяющий общую сложность. Он задает количество итераций основного алгоритма. Память, требуемая для вычисления, пропорциональна значению **N**.
- ▶ **Особенность:** Удвоение значения **N** не просто удваивает время работы, а увеличивает его примерно в 4 раза (так как увеличивает и количество итераций, и объем памяти).

2. `r (blockSize)` – Размер блока

- ▶ **Что это?** Определяет размер блока, на который делится память для обработки. Влияет на общий объем используемой памяти.
- ▶ **На практике:** Обычно устанавливается в 8.

3. **p** (parallelization) – Фактор параллелизма

- ▶ **Что это?** Определяет количество независимых потоков вычислений. Увеличение **p** повышает нагрузку на CPU, не затрагивая использование памяти.
- ▶ **Важно:** Для большинства сценариев верификации пароля, которые являются последовательными операциями, его устанавливают в 1.

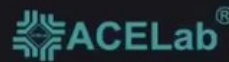
SCRIPT РАССЧЁТЫ

- ▶ Память = $(N + p + 2) * r * 128$ байт.
- ▶ Asic – 1024:1:1 – 130 Кб
- ▶ Android PFE – 2048:8:1 – 2 Мб
Android FDE – 32768:8:1 – 32 Мб

РЕЗУЛЬТАТЫ ТЕСТОВ

### Windows 10		
Node	Threads	Script (N=2048, r=8, p=2)
-----	-----	-----
Ryzen 9 9950X + 2*Nvidia 4060Ti	16/32 + 8704	5125 P/s
Nvidia 4060Ti	4352	1482 P/s
Ryzen 7 5800X + Nvidia 3080Ti	8/16 + 10240 (44%)	2454 P/s
Nvidia 3080Ti		1728 P/s
Ryzen 7 2700 + Nvidia 2060 SUPER	8/16 + 2176	1592 P/s
Nvidia 2060 SUPER	2176	900 P/s
i5-9400F + Nvidia 3060	6/6 + 3584	1180 P/s
Nvidia 3060	3584	776 P/s
Core Ultra 9 285K	24/24	2826 P/s
Ryzen 9 9950X	16/32	2250 P/s
Ryzen 7 7700X	8/16	1065 P/s
Ryzen 7 8845H (laptop)	8/16	945 P/s
Ryzen 7 5800X	8/16	726 P/s
Ryzen 7 5800H (laptop)	8/16	573 P/s
Ryzen 7 6800H (laptop)	8/16	499 P/s
Ryzen 5 5600G	6/12	491 P/s
Ryzen 5 3600X	6/12	465 P/s
Ryzen 5 5500u (laptop)	6/12	408 P/s
i5-9400F	6/6	404 P/s
### Ununtu 24.04		
Node	Threads	Script (N=2048, r=8, p=2)
-----	-----	-----
Ryzen 9 9950X + 2*Nvidia 4060Ti	16/32 + 8704	7456 P/s
Ryzen 9 9950X	16/32	4240 P/s
Core Ultra 9 285K	24/24	4226 P/s

ВРЕМЯ НА РЕШЕНИЕ ЗАДАЧИ



- ▶ $95^8 = 6\,634\,204\,312\,890\,625$.
- ▶ При скорости 20 000 паролей/сек.
- ▶ 10 518 лет.