MOSCOW FORENSICS DAY '25



VYACHESLAV CHIKIN

"SPECIFICS OF ACCELERATING PASSWORD BRUTE-FORCING ON MOBILE DEVICES"

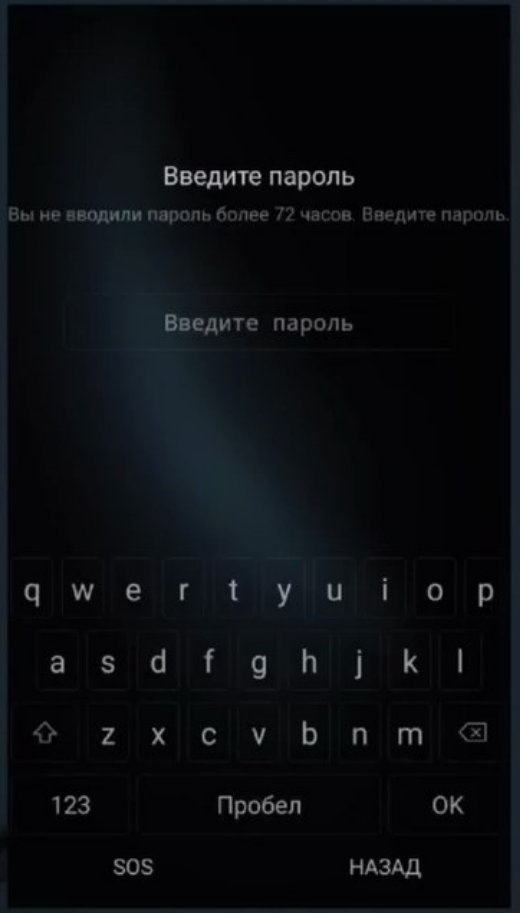
ACELAB

MFD

THE TASK

ACELab®

Crack an 8-character password



2025

POSSIBLE CHARACTERS

ACELab®

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

TOTAL: 95 possible characters

KEYBOARD SPECIFICS

- · → "
- ź → z
- ♡ → e

2025

COMMON ALGORITHMS

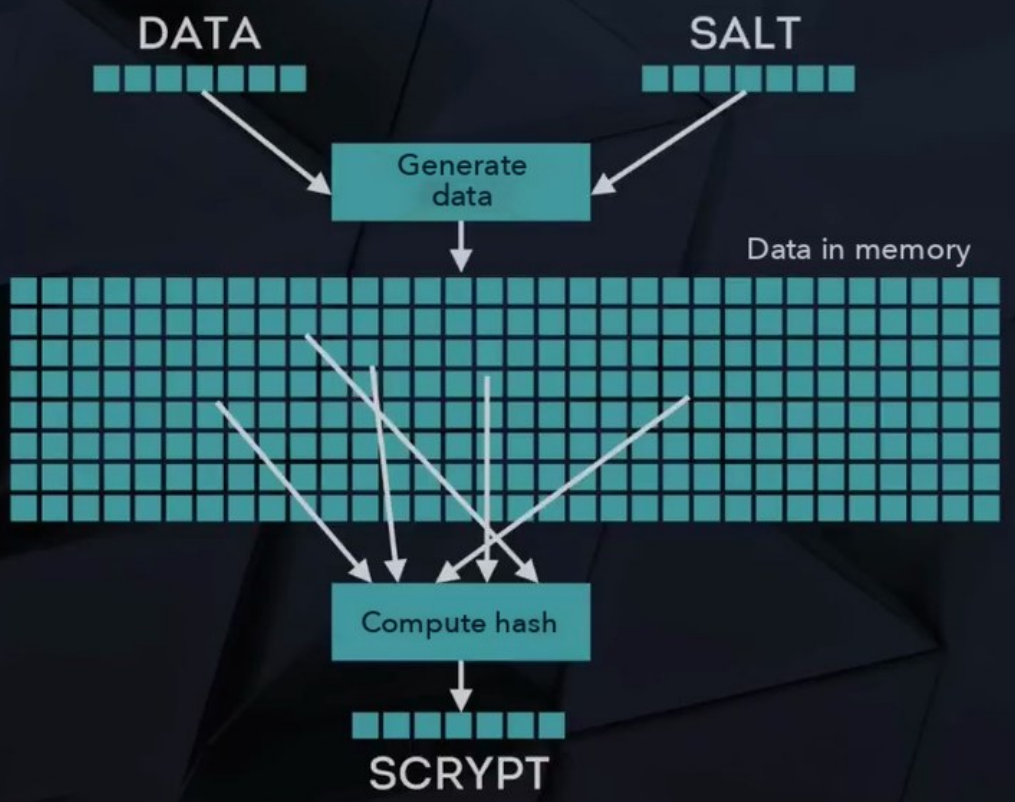
ACELab®

- SHA256
- SCRYPT

2025

HOW SCRYPT WORKS

ACELab®



2025

SCRYPT

ACELab®

1. N (cost factor) - CPU/memory cost factor

- What is it? The main parameter, it sets the overall difficulty. It defines the number of iterations of the core algorithm. The memory required for the computation is proportional to N.
- Note: doubling N does not just double the run time, it increases it about fourfold (it raises both the iteration count and the memory).

SCRYPT

ACELab®

2. r (blockSize) - Block size

- What is it? Sets the size of the block the memory is split into for processing. Affects the total memory used.
- In practice:
  Usually set to 8.

SCRYPT

ACELab®

3. p (parallelization) - Parallelization factor

- What is it? Sets the number of independent computation threads. Raising p loads the CPU without affecting memory use.

- Important: for most password verification scenarios, which are sequential operations, it is set to 1.

SCRYPT CALCULATIONS

ACELab®

- Memory = (N + p + 2) * r * 128 bytes.
- Asic - 1024:1:1 - 130 KB

Android PFE - 2048:8:1 - 2 MB

Android FDE - 32768:8:1 - 32 MB

TEST RESULTS

ACELab®

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

2025

TIME TO SOLVE THE TASK

ACELab®

- 95^8 = 6 634 204 312 890 625.
- At a rate of 20,000 passwords/sec.
- 10,518 years.