ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

Кваліфікаційна робота
на тему:
«Методи та алгоритми хешування паролів на платформі .NET»
Другий (магістерський) рівень

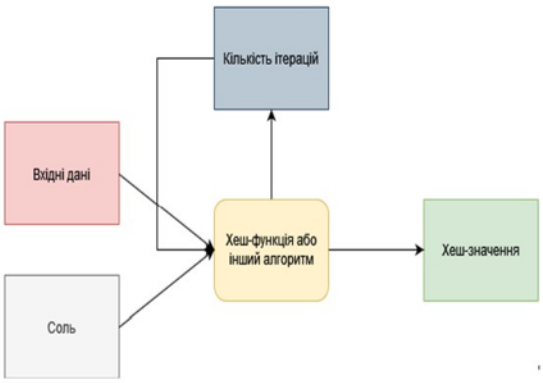
Автор: ст. гр. СПм21-1 Моруга Д.І.
Керівник: доц. Федорченко В.М.

Мета і задачі роботи

- Мета: дослідити методи та алгоритми хешування паролів які доступні для використання на програмній платформі .NET.
- Задачі:
  - Дослідження алгоритмів хешування паролів, вбудованих до програмної платформи .NET;
  - Виявлення та дослідження алгоритмів хешування паролів, які мають реалізації для програмної платформи . NET;
  - Аналіз швидкості та захищеності обраних алгоритмів;
  - Вибір оптимального алгоритму для хешування паролів на програмній платформі .NET.

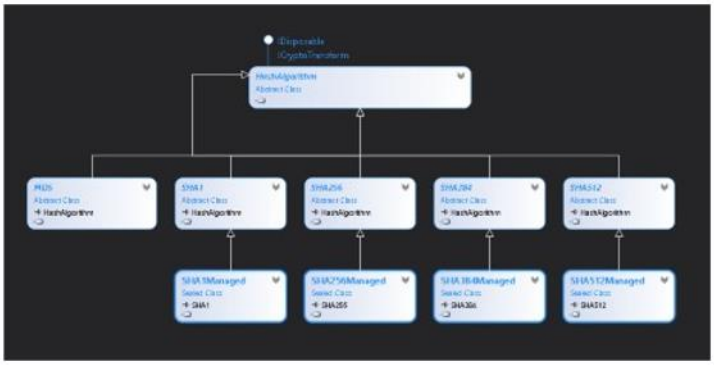
Методи хешування

- Хеш-функція;
- Функція формування ключа



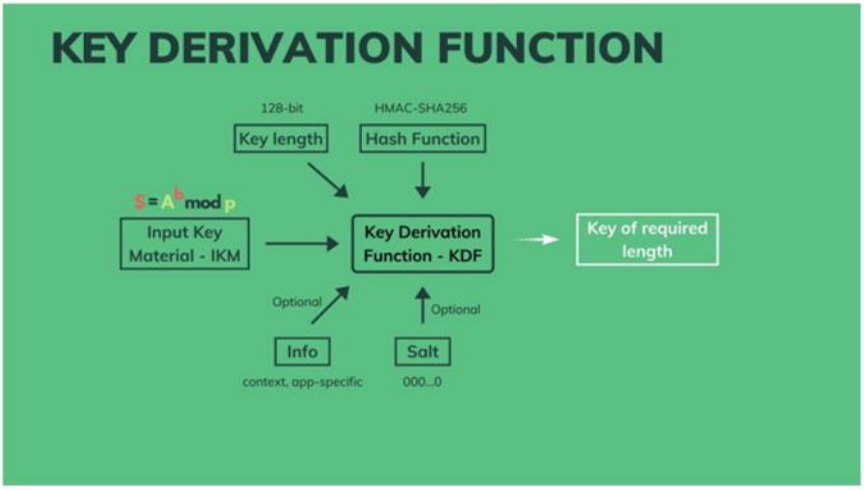
Алгоритми хешування вбудовані до програмної платформи .NET

- MD5;
- SHA;
- PBKDF2.

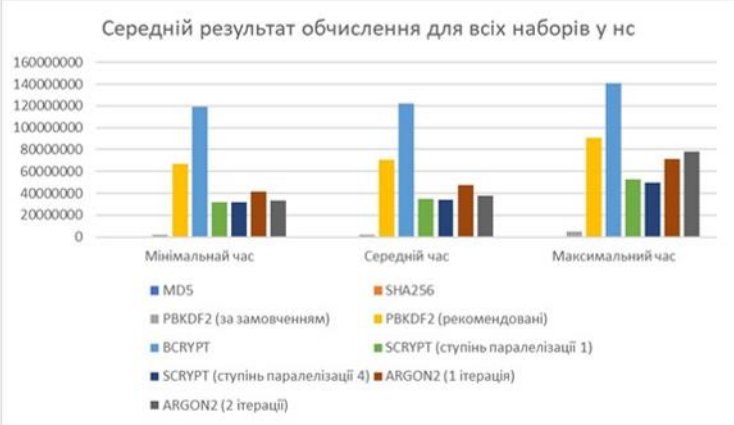


Алгоритми хешування доступні у бібліотеках програмної платформи .NET

- Bcrypt;
- Scrypt;
- Argon2.



Швидкість алгоритмів хешування



Наданий захист

	Атака з райдужною таблицею (наявність солі)	Атака перебором (сповільнення функції)	Захист відGPU	Захист від FPGA/ASIC	Безпека реалізації
MD5	Ні	Ні	Ні	Ні	Так
SHA256	Ні	Ні	Ні	Ні	Так
PBKDF2	Так	Так	Ні	Ні	Так
Bcrypt	Так	Так	Так	Ні	Так
Scrypt	Так	Так	Так	Так	Ні
Argon2	Так	Так	Так	Так	Так

Висновки

- Рекомендовані алгоритми:
  - Argon2 має оптимальну швидкодію, забезпечує захист від GPU, ASIC та FPGA;
  - Bcrypt повільний, забезпечує захист від GPU;
  - PBKDF2 швидкий, відповідає стандарту FIPS-140.
- Нерекомендовані алгоритми:
  - Scrypt немає популярних реалізацій на платформі, потребує багато ресурсів;
  - MD5, SHA відсутній захист від атак за словником, надто швидкі для сучасного обладнання.

ДОДАТОК Б

Детальний аналіз швидкості обчислення хеш-значень

Б.1 Набір 1, 500 найгірших паролів.

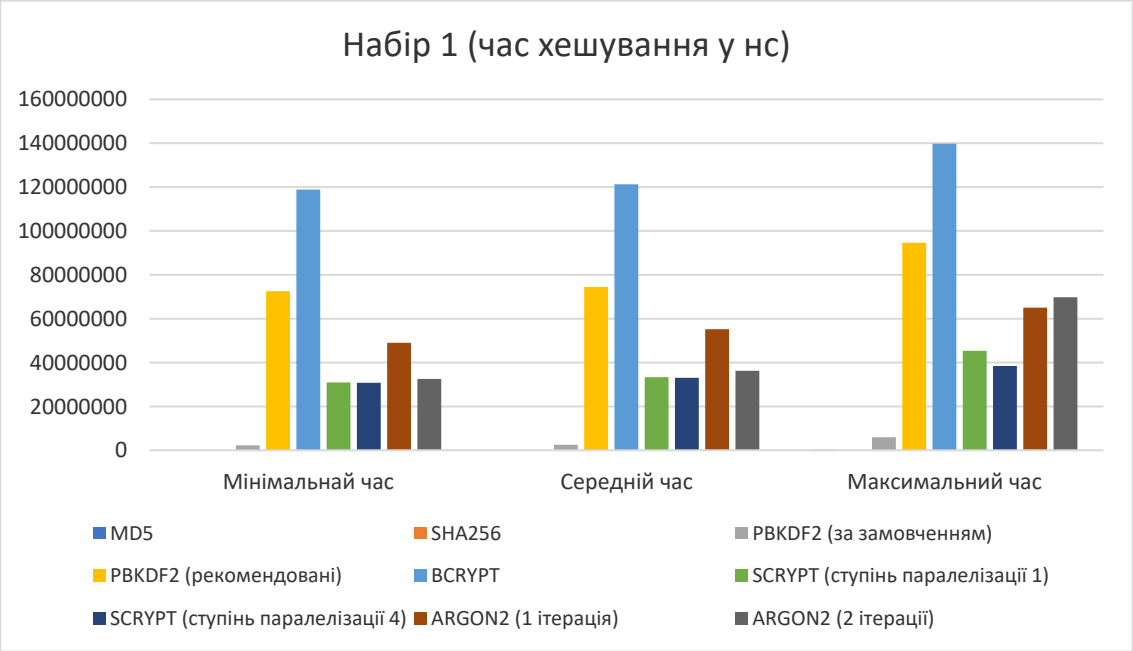


Рисунок Б.1 – Швидкості хешування паролів з набору 1.

Таблиця Б.1 – Метрики обчислення хеш-значень у наносекундах

	Мінімальний час	Середній час	Максимальний час
MD5	300	992	318900
SHA256	200	309	21400
PBKDF2 (за замовченням)	2220200	2547561	5978200
PBKDF2 (рекомендовані)	72505800	74436813	94622600
BCRYPT	118865900	121244886	139751800

Продовження таблиці Б.1

SCRYPT (ступінь паралелізації 1)	30917300	33333892	45361100
SCRYPT (ступінь паралелізації 4)	30807600	33064157	38414500
ARGON2 (1 ітерація)	49035300	55186959	65053299
ARGON2 (2 ітерації)	32533800	36231607	69780000

Б.2 Набір 1, 10000 найбільш поширених паролів.

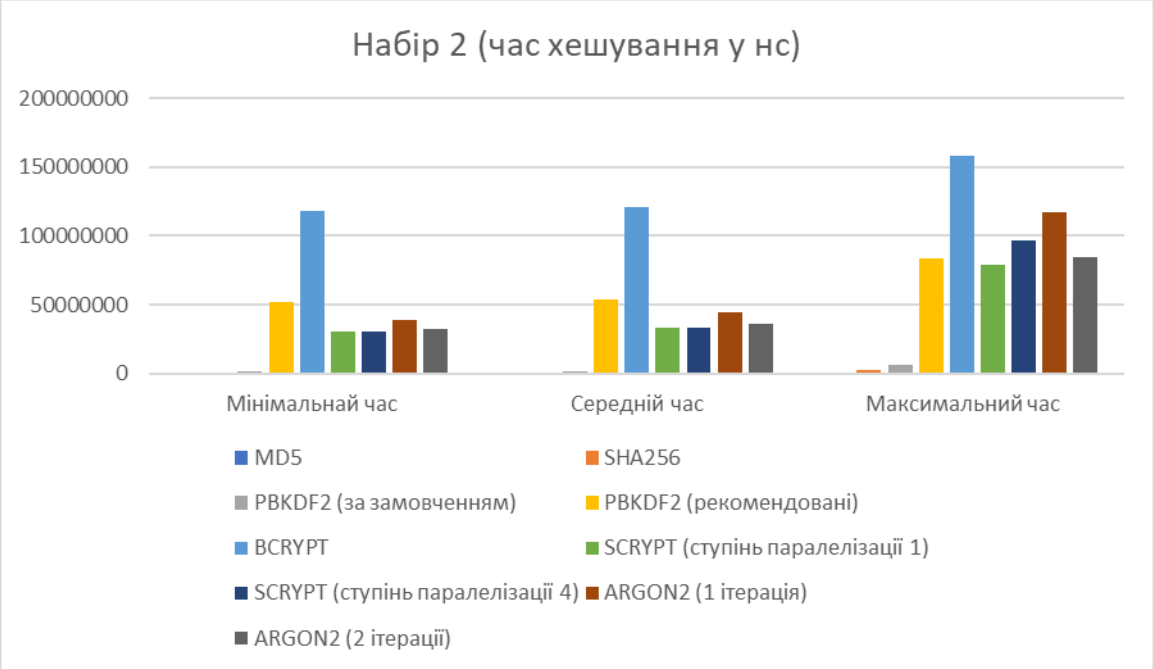


Рисунок Б.2 – Швидкості хешування паролів з набору 2.

Таблиця Б.2 – Метрики обчислення хеш-значень у наносекундах

	Мінімальний час	Середній час	Максимальний час
MD5	200	349	354000

Продовження таблиці Б.2

SHA256	100	447	2567100
PBKDF2 (за замовченням)	2227800	2273545	2434400
PBKDF2 (рекомендовані)	51863000	53602277	83697200
BCRYPT	117780000	120612248	158537900
SCRYPT (ступінь паралелізації 1)	30479400	33244340	79320600
SCRYPT (ступінь паралелізації 4)	30625400	33089827	96382900
ARGON2 (1 ітерація)	38727700	44421589	117271600
ARGON2 (2 ітерації)	32503900	36104959	84467000

Б.3 Набір 3, 20 згенерованих паролів довжиною 8 символів.

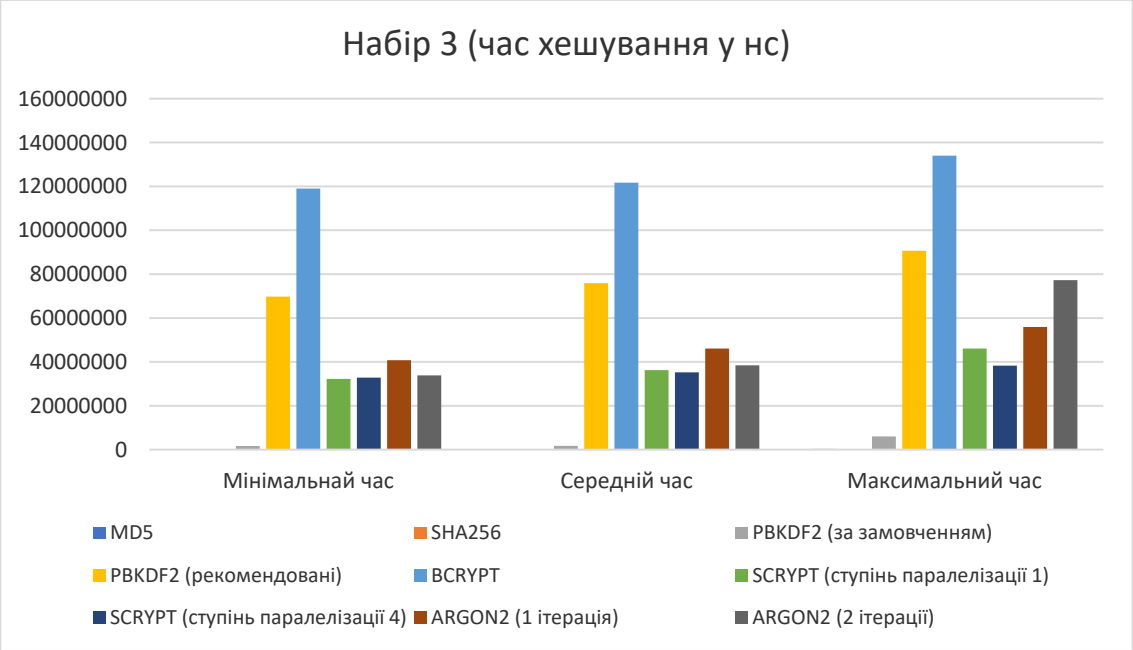


Рисунок Б.3 – Швидкості хешування паролів з набору 3.

Таблиця Б.3 – Метрики обчислення хеш-значень у наносекундах

	Мінімальний час	Середній час	Максимальний час
MD5	300	17955	339300
SHA256	200	1475	23500
PBKDF2 (за замовченням)	2263800	2408600	3404200
PBKDF2 (рекомендовані)	69733400	75886885	90661900
BCRYPT	119035600	121730575	134002299
SCRYPT (ступінь паралелізації 1)	32238700	36260875	46072000
SCRYPT (ступінь паралелізації 4)	32170700	34477240	38395700

Продовження таблиці Б.3

ARGON2 (1 ітерація)	40810200	46094510	55958900
ARGON2 (2 ітерації)	33879600	38464470	77274800

Б.4 Набір 4, 20 згенерованих паролів довжиною 12 символів.

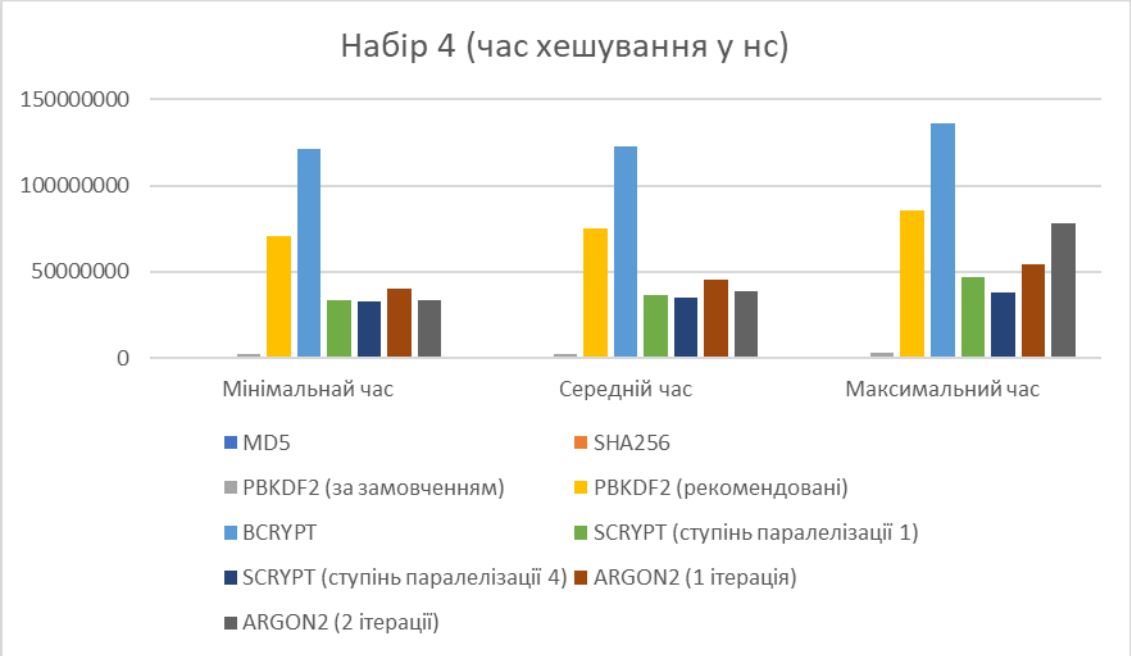


Рисунок Б.4 – Швидкості хешування паролів з набору 4.

Таблиця Б.4 – Метрики обчислення хеш-значень у наносекундах

	Мінімальний час	Середній час	Максимальний час
MD5	500	29585	553700
PBKDF2 (за замовченням)	2222300	2420100	3430100
PBKDF2 (рекомендовані)	70871900	75097515	85886300

Продовження таблиці Б.4

BCRYPT	121514000	123011580	136366400
SCRYPT (ступінь паралелізації 1)	33544400	36337740	47112900
SCRYPT (ступінь паралелізації 4)	32850100	35210400	38304000
ARGON2 (1 ітерація)	40070500	45542595	54311900
ARGON2 (2 ітерації)	33447100	38872420	77859600

Б.5 Набір 5, 20 згенерованих паролів довжиною 15 символів.

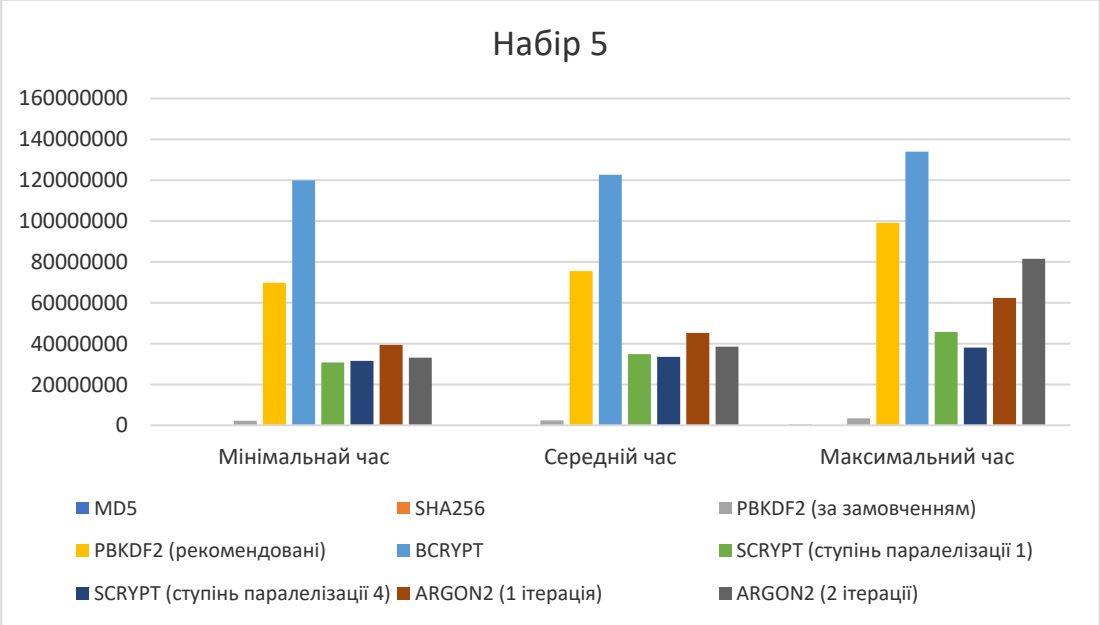


Рисунок Б.5 – Швидкості хешування паролів з набору 5.

Таблиця Б.5 – Метрики обчислення хеш-значень у наносекундах

	Мінімальний час	Середній час	Максимальний час

Продовження таблиці Б.5

MD5	300	21330	410300
SHA256	200	1305	20500
PBKDF2 (за замовченням)	2220200	2547561	5978200
PBKDF2 (рекомендовані)	69831300	75489015	99097600
BCRYPT	119918800	122620645	133958899
SCRYPT (ступінь паралелізації 1)	30785300	34862115	45756900
SCRYPT (ступінь паралелізації 4)	31571099	33505979	38073100
ARGON2 (1 ітерація)	39409900	45259335	62383600
ARGON2 (2 ітерації)	33168999	38497620	81493000

ДОДАТОК В

Детальні результати атак

В.1 MD5.

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: D:\Diploma\HashComparison\Hashes\MD5\500-worst.txt
Time.Started.....: Wed Nov 23 12:20:29 2022 (3 secs)
Time.Estimated...: Wed Nov 23 12:20:32 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (C:\Users\trluxus\Downloads\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5557.4 kH/s (3.03ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered........: 497/499 (99.60%) Digests (total), 497/499 (99.60%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[30383533333636313433] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 56c Util: 31% Core:1809MHz Mem:5989MHz Bus:8
```

Рисунок В.1 – Атака за словником набір 1.

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: D:\Diploma\HashComparison\Hashes\MD5\10k-popular.txt
Time.Started.....: Wed Nov 23 12:22:13 2022 (30 secs)
Time.Estimated...: Wed Nov 23 12:22:43 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (C:\Users\trluxus\Downloads\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   476.2 kH/s (3.15ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered........: 9471/10000 (94.71%) Digests (total), 9471/10000 (94.71%) Digests (new)
Remaining........: 529 (5.29%) Digests
Recovered/Time...: CUR:N/A,N/A,N/A AVG:N/A,N/A,N/A (Min,Hour,Day)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[30383533333636313433] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 55c Util: 31% Core:1350MHz Mem:4565MHz Bus:8
```

Рисунок В.2 – Атака за словником набір 2.

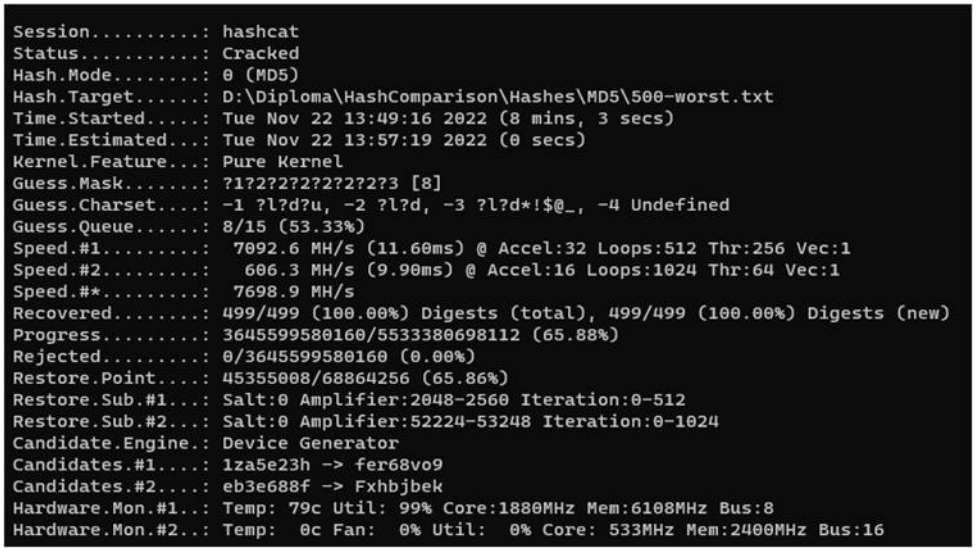


Рисунок В.3 – Атака методом повного перебору набір 1.

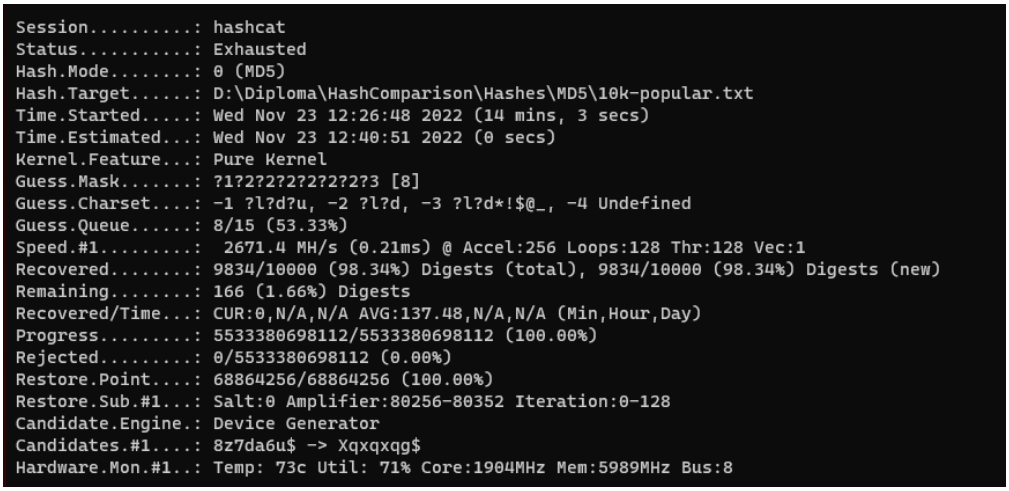


Рисунок В.4 Атака методом повного перебору набір 2.

В.2 SHA256.

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: D:\Diploma\HashComparison\Hashes\MD5\500-worst.txt
Time.Started.....: Wed Nov 23 12:20:29 2022 (3 secs)
Time.Estimated...: Wed Nov 23 12:20:32 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (C:\Users\trluxus\Downloads\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5557.4 kH/s (3.03ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered........: 497/499 (99.60%) Digests (total), 497/499 (99.60%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[30383533333636313433] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 56c Util: 31% Core:1809MHz Mem:5989MHz Bus:8
```

Рисунок В.5 – Атака за словником набір 1.

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: D:\Diploma\HashComparison\Hashes\MD5\10k-popular.txt
Time.Started.....: Wed Nov 23 12:22:13 2022 (30 secs)
Time.Estimated...: Wed Nov 23 12:22:43 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (C:\Users\trluxus\Downloads\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   476.2 kH/s (3.15ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered........: 9471/10000 (94.71%) Digests (total), 9471/10000 (94.71%) Digests (new)
Remaining........: 529 (5.29%) Digests
Recovered/Time...: CUR:N/A,N/A,N/A AVG:N/A,N/A,N/A (Min,Hour,Day)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[30383533333636313433] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 55c Util: 31% Core:1350MHz Mem:4565MHz Bus:8
```

Рисунок В.6 – Атака за словником набір 2.

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: D:\Diploma\HashComparison\Hashes\MD5\500-worst.txt
Time.Started.....: Tue Nov 22 13:49:16 2022 (8 mins, 3 secs)
Time.Estimated...: Tue Nov 22 13:57:19 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?2?2?2?2?2?3 [8]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 8/15 (53.33%)
Speed.#1.........:  7092.6 MH/s (11.60ms) @ Accel:32 Loops:512 Thr:256 Vec:1
Speed.#2.........:   606.3 MH/s (9.90ms) @ Accel:16 Loops:1024 Thr:64 Vec:1
Speed.#*.........:  7698.9 MH/s
Recovered........: 499/499 (100.00%) Digests (total), 499/499 (100.00%) Digests (new)
Progress.........: 3645599580160/5533380698112 (65.88%)
Rejected.........: 0/3645599580160 (0.00%)
Restore.Point....: 45355008/68864256 (65.86%)
Restore.Sub.#1...: Salt:0 Amplifier:2048-2560 Iteration:0-512
Restore.Sub.#2...: Salt:0 Amplifier:52224-53248 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1....: 1za5e23h -> fer68vo9
Candidates.#2....: eb3e688f -> Fxhbjbek
Hardware.Mon.#1..: Temp: 79c Util: 99% Core:1880MHz Mem:6108MHz Bus:8
Hardware.Mon.#2..: Temp:  0c Fan:  0% Util:  0% Core: 533MHz Mem:2400MHz Bus:16
```

Рисунок В.7 – Атака методом повного перебору набір 1.

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: D:\Diploma\HashComparison\Hashes\MD5\10k-popular.txt
Time.Started.....: Wed Nov 23 12:26:48 2022 (14 mins, 3 secs)
Time.Estimated...: Wed Nov 23 12:40:51 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?2?2?2?2?2?3 [8]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 8/15 (53.33%)
Speed.#1.........:  2671.4 MH/s (0.21ms) @ Accel:256 Loops:128 Thr:128 Vec:1
Recovered........: 9834/10000 (98.34%) Digests (total), 9834/10000 (98.34%) Digests (new)
Remaining........: 166 (1.66%) Digests
Recovered/Time...: CUR:0,N/A,N/A AVG:137.48,N/A,N/A (Min,Hour,Day)
Progress.........: 5533380698112/5533380698112 (100.00%)
Rejected.........: 0/5533380698112 (0.00%)
Restore.Point....: 68864256/68864256 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:80256-80352 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: 8z7da6u$ -> Xqxqxqg$
Hardware.Mon.#1..: Temp: 73c Util: 71% Core:1904MHz Mem:5989MHz Bus:8
```

Рисунок В.8 Атака методом повного перебору набір 2.

В.3 BCRYPT.

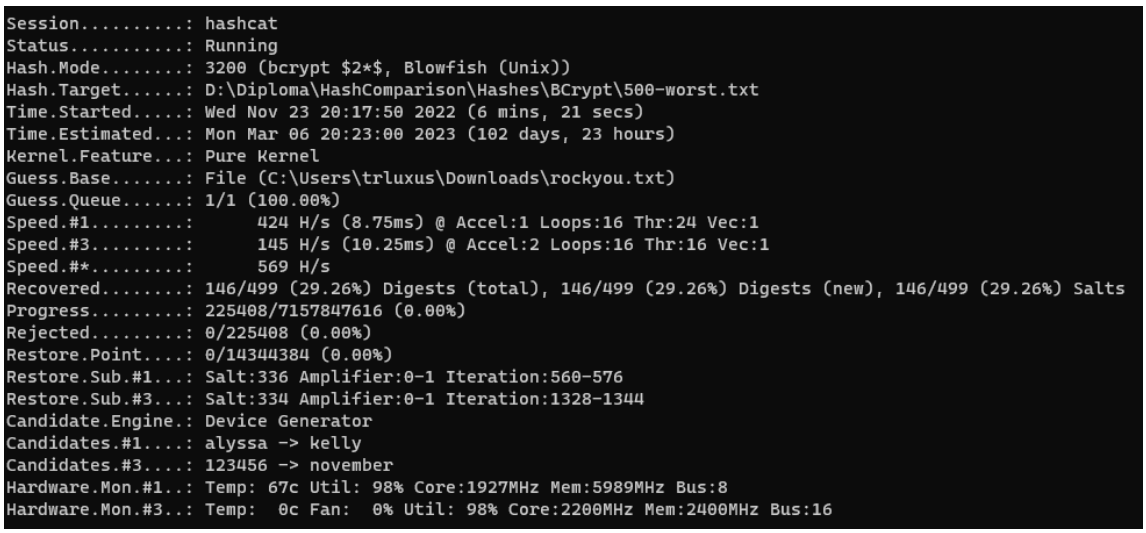


Рисунок В.9 – Атака за словником набір 1.