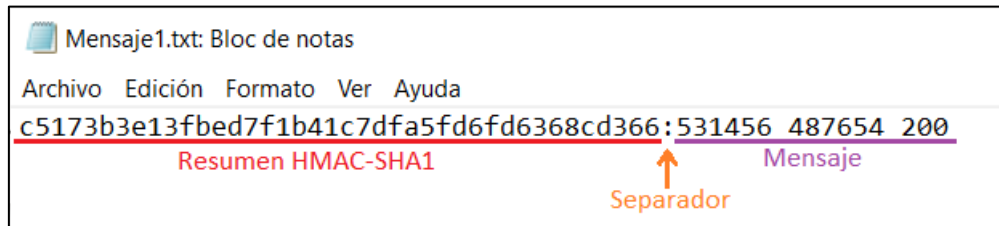


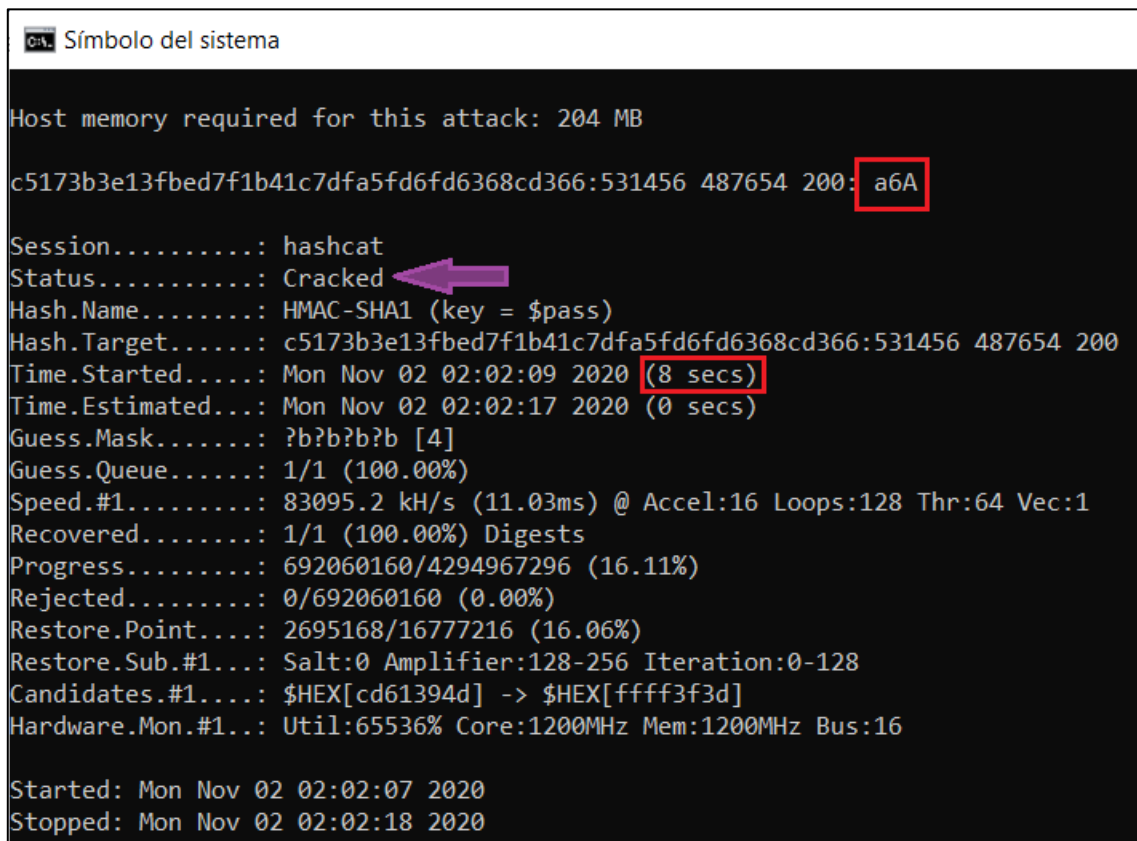
Apartado a.



Formato para usar Hashcat

```
D:\Escritorio\UNI\SSII\hashcat-6.1.1>hashcat.exe -m 150 -a 3 D:\Escritorio\UNI\SSII\Consultoria2\Mensaje1.txt ?b?b?b?b
hashcat (v6.1.1) starting...
```

Comando usado para obtener la clave



Obtención de clave del primer mensaje

```
Símbolo del sistema

Host memory required for this attack: 204 MB

158413dd62eada5273a72f9fa35f4e19ddb864b8:541157 487655 200:$HEX[21ae2d41]

Session.....: hashcat
Status.....: Cracked ←
Hash.Name.....: HMAC-SHA1 (key = $pass)
Hash.Target.....: 158413dd62eada5273a72f9fa35f4e19ddb864b8:541157 487655 200
Time.Started.....: Mon Nov 02 02:29:29 2020 (7 secs)
Time.Estimated...: Mon Nov 02 02:29:36 2020 (0 secs)
Guess.Mask.....: ?b?b?b?b [4]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 83287.9 kH/s (11.02ms) @ Accel:16 Loops:128 Thr:64 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 623902720/4294967296 (14.53%)
Rejected.....: 0/623902720 (0.00%)
Restore.Point....: 2433024/16777216 (14.50%)
Restore.Sub.#1...: Salt:0 Amplifier:0-128 Iteration:0-128
Candidates.#1....: $HEX[7361392e] -> $HEX[d2ff3f37]
Hardware.Mon.#1..: Util:65536% Core: 200MHz Mem:1200MHz Bus:16

Started: Mon Nov 02 02:29:27 2020
Stopped: Mon Nov 02 02:29:37 2020
```

Obtención de clave del segundo mensaje

Conversión de Hexadecimal a ASCII:

21ae2d41 (Hex) → !®-A

Apartado b.

Pruebas: Sin cambiar la longitud de la primera clave (4 bytes), solo el algoritmo de encriptado.

HMAC-SHA256 con clave “ a6A”

```
5
6 public class MAC {
7
8     static String alg = "HmacSHA256";
9
10 public static void main(String[] args) {
11     String msg = "531456 487654 200";
12     System.out.println("Mensaje : " + msg);
13     byte[] decodedKey = {32,97,54,65}; ← Clave (espacio)a6A en decimal
14     String resumen = performMACTest(msg, decodedKey);
15     System.out.println("Clave Hex : "
16         + byteArrayToHexString(decodedKey) + "\t\tString : "
17         + new String(decodedKey));
18     System.out.println("MAC : " + resumen);
19 }
20
21 public static String performMACTest(String s, byte[] decodedKey) {
22     String st = "";
23     try {
24         Mac mac = Mac.getInstance(alg);
25         SecretKey key = new SecretKeySpec(decodedKey, 0, decodedKey.length,
26             alg);
27         mac.init(key);
28         mac.update(s.getBytes());
29         byte[] b = mac.doFinal();
30         st = byteArrayToHexString(b);
31     } catch (Exception e) {
32         System.out.println(e.getMessage());
33     }
34     return st;
35 }
36
```

< Problems @ Javadoc Declaration Console

<terminated> MAC [Java Application] C:\Program Files\Java\jdk-11.0.4\bin\javaw.exe (3 nov. 2020 0:44:51 – 0:44:51)

Mensaje	: 531456 487654 200
Clave Hex	: 20613641 String : a6A
MAC	: d9067c92615f62ef4f63314956b2555fe0e6b8e18427cb7a2b25d51feae91593

Generación nuevo resumen con HMAC-SHA256

```
Símbolo del sistema
d9067c92615f62ef4f63314956b2555fe0e6b8e18427cb7a2b25d51feae91593:531456 487654 200: a6A
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: HMAC-SHA256 (key = $pass)
Hash.Target.....: d9067c92615f62ef4f63314956b2555fe0e6b8e18427cb7a2b2...54 200
Time.Started.....: Tue Nov 03 00:48:53 2020 (28 secs)
Time.Estimated...: Tue Nov 03 00:49:21 2020 (0 secs)
Guess.Mask.....: ?b?b?b?b [4]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 25027.7 kH/s (9.04ms) @ Accel:8 Loops:64 Thr:64 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 691011584/4294967296 (16.09%)
Rejected.....: 0/691011584 (0.00%)
Restore.Point....: 2695168/16777216 (16.06%)
Restore.Sub.#1...: Salt:0 Amplifier:192-256 Iteration:0-64
Candidates.#1....: $HEX[8261394d] -> $HEX[ffff2f77]
Hardware.Mon.#1..: Util:65536% Core: 200MHz Mem:1200MHz Bus:16

Started: Tue Nov 03 00:48:33 2020
Stopped: Tue Nov 03 00:49:22 2020
```

Obtención primera clave con HMAC-SHA256

Tiempo = 28 segundos

Ligera mejora respecto a los 8 segundos con HMAC-SHA1, pero insignificante a nivel de seguridad.

HMAC-SHA512 con clave “ a6A”

Mensaje	: 531456 487654 200
Clave Hex	: 20613641 String : a6A
MAC	: a7eb5acba06330057aca3b0a01d4abbcab987e0a44030e4c7aef008dbfaa83736185216756e3df309969e228c27fdd7a35c05b09dc9303f69babecff300a40c8

Generación nuevo resumen con HMAC-SHA512

Para HMAC-SHA512 con la misma clave, 4 bytes, tarda bastante más tiempo. No medido. Podría ser el límite, y ser insegura y descifrable con tiempo, por lo que recomendamos aumentar el número de bytes a 5 o 6, garantizando la seguridad.