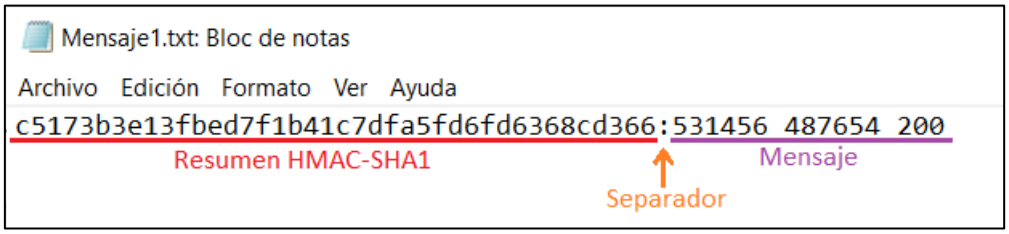
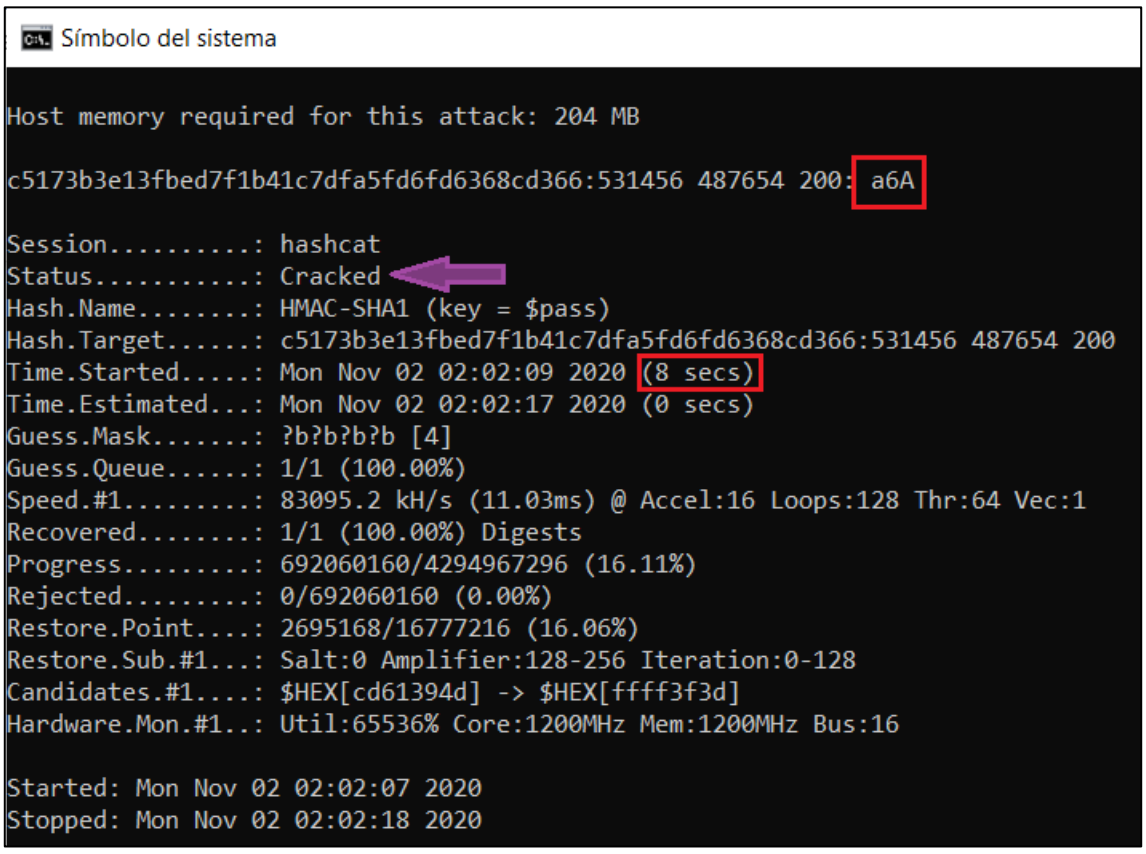
Apartado a.



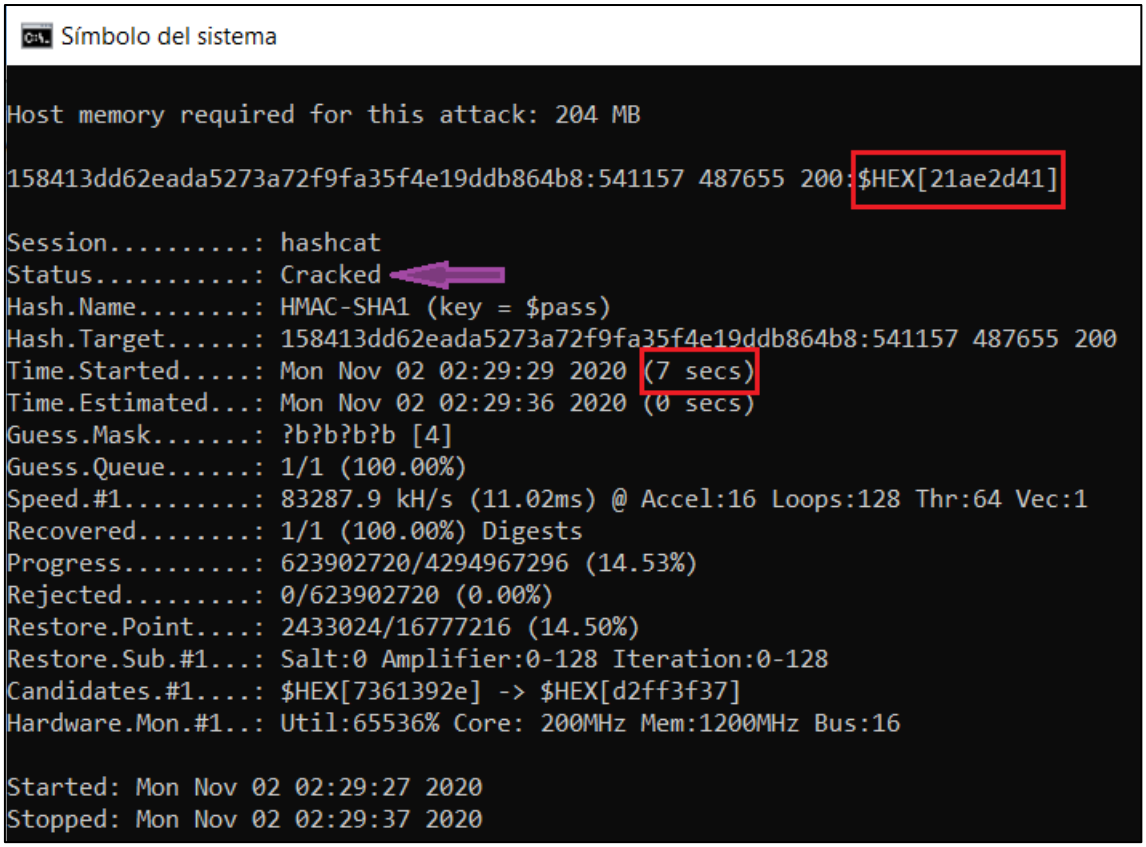
Formato para usar Hashcat

```
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



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”

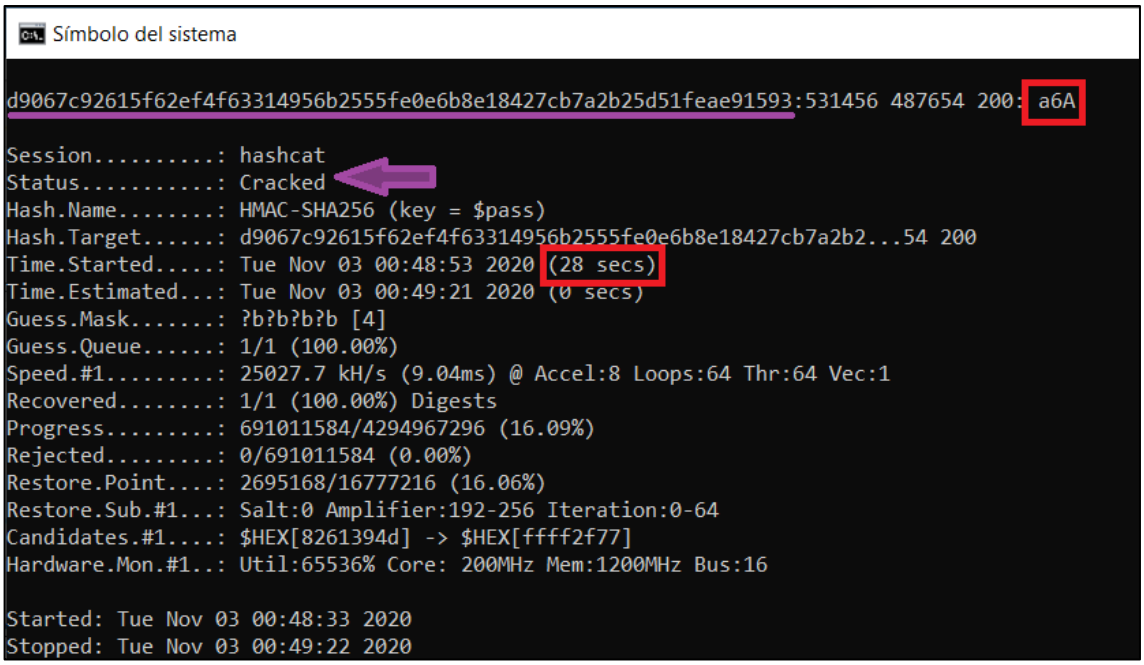
```
5
6  public class MAC {
7
8      static String alg = "HmacSHA256";
9
10     public static void main(String[] args) {
11         String msg = "531456 487654 200";
12         System.out.println("Mensaje          : " + msg);
13         byte[] decodedKey = {32,97,54,65};
14         String resumen = performMACTest(msg, 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
```

Clave (espacio)a6A en decimal

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

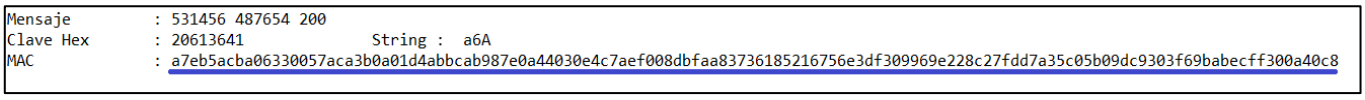


Obtención primera clave con HMAC-SHA256

Tiempo = 28 segundos

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

HMAC-SHA512 con clave “ a6A”



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.