# ONE WAY HASH FUNCTION

Av Evan Saboo – saboo@kth.se

# ONE WAY HASH FUNCTION

Av Evan Saboo – saboo@kth.se

# Uppgift 1.

### Fråga 1.1:

Skillnaden mellan algoritmerna är längden: Man kan se direkt att MD5 är har den minsta längden av alla 3 hash funktionerna, sedan kommer SH1 och till sista har SH256 den längsta hashen. MD5 har 32 karaktärer, SHA1 har 40 karaktärer och SHA256 har 64 karaktärer. Man kan också se att alla karaktärer i varje hash har bara karaktären 0 till 9 och a till f, vilket betyder att alla hasher representeras som hexadecimal.

### Fråga 2.2:

MD5= 2b35ddc8da488848ebc90b58ab3d3ab6

SHA1= f02b03b3619788d92b2f82a31d004d516007185d

SHA256= 7b2eb668d467b05f8338a5eb57b9f0741c625565af9affee831b65d315976ac0

# Uppgift 2.

### Fråga 2.3:

Jag testade med flera nycklar (från en karaktär till 64 karaktären) och även den största nyckeln fungerar med alla hash-funktioner.
Men efter en del efterforskningar fick jag veta att varje hash-funktion har sin egen HMAC gräns.

MD5 har ca. $2^{32}$ bits HMAC gräns.

SHA1 och SHA256 har ca. $2^{64}$ bits HMAC gräns.

### Fråga 2.4:

HMAC-MD5= 7fce5c5f3c56c982ab5a47c0984313a1

HMAC-SHA1= 3f01a9f71857553ff5265333dc4e35d4c72922b7

HMAC-SHA256= 591dc585415ba3b262e2a3ad95a6bbfe09d336e9da33f47139606fe2e176e3b0

# Uppgift 3.

Fråga 3:

Om man flippar sista biten i texten "saboo@kth.se" ("01100001" -> "11100001") omvandlas det till "áaboo@kth.se"

---

SHA1= f02b03b3619788d92b2f82a31d004d516007185d

Blir till ->

SHA1= 8ceee8c5a674b76b06bb59421bfd016d385f3cb2

---

SHA256= 7b2eb668d467b05f8338a5eb57b9f0741c625565af9affee831b65d315976ac0

Blir till ->

SHA256= d54a5272b8de476bb14c3c69ef33dccbdd4330695b9be85ddae9de2e930585ae

---

Om man jämför alla hash functions kan man se att även om man ändrar minst en bokstav kommer hela hash functionen att ändras.

## Fråga 3.5:

I observationen har jag räknat ut att det är 52 bitar som är likadana i MD hashen, och 126 bitar var likadana mellan vanliga hashen och den modifierade hashen.

MD5 = 52 bitar

SH256 = 126 bitar

# Uppgift 4.

Fråga 4.6:

IV1013-key = 37 952 190 tries

Security is fun = 37 892 752 tries

Yes, indeed = 10 460 932 tries

Secure IV1013 = 10 532 906 tries

No way = 18 745 851 tries