**1.**

Noekkelen er: “a0b271a9d8aa8e7473922164d6a1c03c”.

Ulempen ved symmetrisk kryptering er at det er svært risikabelt å sende nøkkelen i klartekst over usikre kanaler.

**2.**

Passordet er: “Pterodactylus”

MD5 ble brukt til å hashe passordet. Problemet med MD5 er at den ikke er kollisjons-resistent. Dvs. to inputs kan gi samme hash-verdi.

**3.**

Kodenavnene er:

* *BigBearBrontosaurus*
* *RaptorBoi99*
* (*Blaise* kan ut fra teksten leses å være en hemmelig agent, men det refereres antageligvis til den Franske krypto-forskeren Blaise de Vigenère)

Nøkkelegenskapene til en hashing-algoritme:

1. Algoritmen må vaere rask

2. Algoritmen må i all praksis være kollisjonsresistent

3. En liten endring i det som endres, maa forårsake enorm endring i dens hash-verdi

4. Den må være tilnærmet umulig å reversere

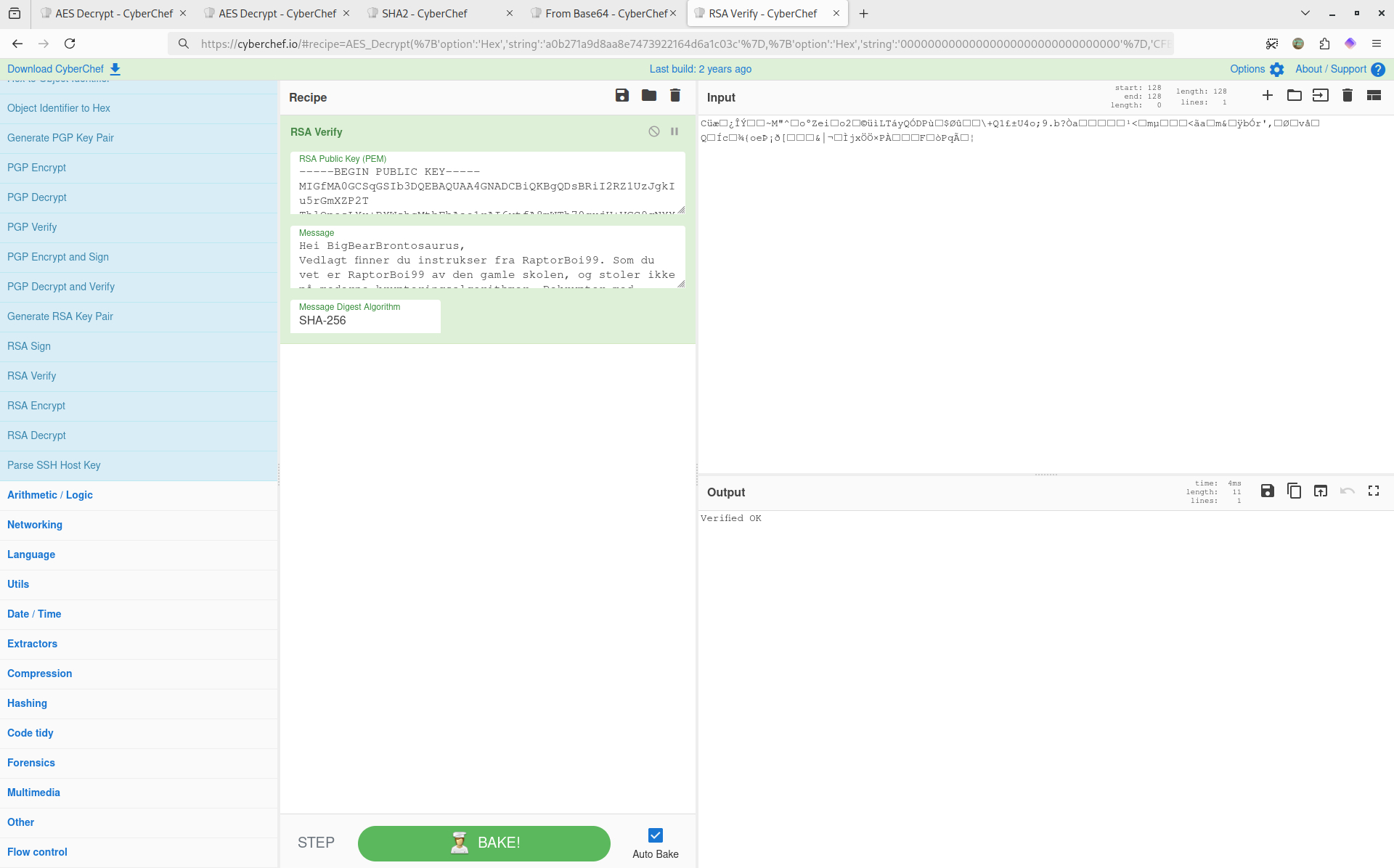
5. Den må være deterministisk

Leveringspunktet er Dana bakeri.

Algoritmen som ble brukt inne i meldingen, heter Vigenère-chifferet, og man knekker det ved å se etter statistiske ujevnheter i det antatte klartekstspråket.

Se under for skjermbilde av den verifiserte meldingen.

Man signerer med sin private nøkkel. Logikken her er at kun undertegneren har tilgang til den private nøkkelen, mens allmennheten har tilgang til den offentlige nøkkelen. En melding som er signert med en privat nøkkel, kan kun verifiseres av dens tilhørende offentlige motpart.



Meldingen ble verifisert uten problemer.