**Encryption**

Encryption is het veranderen van een message of het scrambelen van een message.

Zodat niemand zomaar deze message kan zien. Hier voor moet je de message decrypten

**Decryption**

Decryption is het pakken van de message en deze weer unscrambelen of het weer terug veranderen naar de oorspronkelijke vorm. Zodat je de message kan lezen.

**Caepher’s Cipher:**

Was een van de eerte encryptions. Genoemd naar Julius caephar

Een roman general die zijn berichten encrypten zodat wanneer ze werden onderschept door de vijand deze het bericht niet konden lezen. Caepher’s chiper Is een algoritme die een letter pakt en daar een getal bij pakt en die omlaag gaat in het alfabat. Bijvoorbeeld al je 1 hebt dan krijg je a=b, b=c en zo door wanneer je getal 2 Is dan word het a=c, b=d en zo door. Om het bericht the decrypten moet je het word pakken en dan met een aantal eraf doen. Komt dit op een normale message (leebaar) dan Is het gelukt. (natuurlijk gaat dit makkelijker als je het getal weet dat veranderd omdat er 26 mogelijk combinatie zijn en dit is dus niet erg lasting en zeker niet nu er computers bestaan die dit binnen een fractie van een seconden kunnen doen. Nu kun je alle letter in de zin met een ander getal veranderen dat maakt het

Rond de 10 billion mogelijkheden. Dit zou een normal mens niet lukken om allemaal te proberen.

Maar een computer tegenwordig kan alle 10 billion mogelijkheden binnen een paar seconden doen.

**256 bit keys**

Tegenwordig worden messages met een 256 bit key protect

Die zou een oneindigheid dingen combinaties gebruiken. Om precieser te zijn een getal met 78 getallen erin. Zelfs al zou je honderd duizend super computers hebben die een miljoen biljoen keys kan proberen elke seconden zou het nog trillions of Jaren duren. Voordat het wachtwoord is geraden. Maar computer chips worden elk jaar wel 2x zo snel en ook 2x zo klein. Zou dit uiteindelijk veel sneller gaan en word het dus mogelijk om het binnen no time te decrypten

En zou een 256 bit key niet meer goed genoeg zijn om veilig te zijn.

Er is zelfs al een keer geweest waar ze de bit key moesten vergroten om bij te blijven van de snelle groei van computers. Het maakt de message niet zwaar om te gebruiken maar het veranderd alleen de aantal mogelijke antwoorden.

**Symmetric encryption**

Dit is wanneer de sender en de ontvanger de zelfde key hebben

Daarvoor moet de key worden door gegeven alleen is het onmogelijk voor 2 computers om elkaar prive te ontmoeten. Om de secret key door te geven. Daarom gebruiken mensen een

Asymmetric key die gebruik maakt van een public key die iedereen kan krijgen / ontvangen en een private key die niet word gedeelt de public key word gebruikt voor het encrypten van data en iedereen kan dit gebruiken voor het maken van een secret message. Maar dit kan alleen worden decrypted door een computer die in bezit is van de private key.