Algoritme 1 = OTP

Key = Geen van toepassing

Principewerking: Vervang oude key door een nieuwe cryptographic key te genereren. In het voorbeeld worden de letters vervangen in de plaintext door de letter die 13 letters na de originele letter komt in het alfabet. (alfabet kan ook terug naar het begin gaan bijvoorbeeld z wordt m)

Algoritme 2 = HEX

Key = Niet van toepassing

Principewerking:

Algoritme 3 =Rotation

Key = \*\*\*

Principewerking: ASCII

Algoritme 4 = XOR

Key = …

Principewerking:...

Algoritme 5 = Substitution

Key = Security Essentials

Principewerking: vervangen van characters

Algoritme 6 = Vigenère

Key =  Niet van toepassing

Principewerking:  Het encrypten van alphabetic tekst door gebruik te maken van een serie van interwoven Caeser ciphers.

Algoritme 7 =

Key = Niet van toepassing

Principewerking:

1. OTP
2. **HEX**
3. **Rotation**
4. **XOR**
5. **Substitution**
6. **Vigenère**
7. **Base64**

Algoritme 1 = Substitution

Key = Geen van toepassing

Principewerking: Vervang oude key door een nieuwe cryptographic key te genereren. In het voorbeeld worden de letters vervangen in de plaintext door de letter die 13 letters na de originele letter komt in het alfabet. (alfabet kan ook terug naar het begin gaan bijvoorbeeld z wordt m)

Algoritme 2 = Base64

Key = Niet van toepassing

Principewerking: Base64-codering kan worden toegepast op een willekeurige reeks bytes. Het algoritme voor de codering verwerkt de data in groepjes van drie bytes. Die bevatten 3 × 8 = 24 willekeurige bits. Die worden gehergroepeerd in vier bytes van 6 bits (4 × 6 is ook 24). Elke byte kan dan dus maar zes bits bevatten, de overige worden nul. Dat maakt 64 combinaties mogelijk. De 64 wordt vol gemaakt met het =-teken en de binaire nul. Daarmee kan ook een mouw worden gepast aan data worden omgezet naar leesbare tekens: hoofdletters, kleine letters en cijfers = 2 × 26 + 10 = 62 tekens, plus de slash en het plusteken.

Algoritme 3 =

Key = \*\*\*

Principewerking: ASCII

Algoritme 4 =

Key = …

Principewerking:...

Algoritme 5 = Vigenère

Key = SECURITYESSENTIALS

Principewerking: Men kiest eerst een geheime sleutel in de vorm van een geheim sleutelwoord, bijvoorbeeld ZODIAK. Dit schrijft men onder de klare tekst. Vervolgens zoekt men de klare letter in het verticale alfabet op en de letter van het sleutelwoord in het horizontale alfabet. De kruising van beiden is de resulterende codeletter.

Algoritme 6 = HEX

Key =  Niet van toepassing

Principewerking:  Talstelsel waarbij met tien cijfers wordt gewerkt, maar met zestien cijfers. De cijfers 0 t/m 9 worden daarom uitgebreid met 'A' (=10) t/m 'F' (=15), ook wel 'a' t/m 'f'.

Algoritme 7 = XOR

Key = fedcba987654321

Principewerking: De XOR-operator is zeer gebruikelijk als onderdeel in complexere cijfers. Op zichzelf, met behulp van een constant herhalende sleutel, kan een eenvoudige XOR-codering triviaal worden verbroken met behulp van frequentieanalyse. Als de inhoud van een bericht kan worden geraden of op een andere manier bekend is, kan de sleutel worden onthuld. De belangrijkste verdienste is dat het eenvoudig te implementeren is en dat de XOR-bewerking rekenkundig niet duur is. Een eenvoudig herhalend XOR-cijfer (d.w.z. dezelfde sleutel gebruiken voor xor-bewerkingen op alle gegevens) wordt daarom soms gebruikt om informatie te verbergen in gevallen waarin geen bepaalde beveiliging vereist is. De XOR-codering wordt vaak gebruikt in computermalware om reverse engineering te bemoeilijken.