Opdracht 4: Protecting Secrets

**4.1: Terminology**

|  |  |
| --- | --- |
| Encryption | The process of encoding a message or information so only certain people can access it |
| Decryption | The process of transforming encrypted information so you can understand/read it again |
| Cryptanalysis | The process of deciphering coded messages without knowing the key |
| Algorithm | A process or set of rules to be followed in calculations or problem-solving |
| Key (cryptography) | A piece of information that determines the output of a cryptographic algorithm |
| Steganography | The practice of concealing a file/message/image/video within a file/message/image/video |
| Security through obscurity | The belief that a system of any sort can be secure as long as nobody out of its user group is allowed to find out anything internal |
| Kerckhoff’s principle | The concept that a cryptographic system should be designed to be secure, even if everything except the key is public |
| PKI (public key infrastructure) | A set of roles, policies and procedures which you need to create, manage, distribute, use, store and revoke digital certificates. Also used to manage public-key encryption |
| Brute Force | Guessing passwords until you get the right one. Keeps checking until one is found. |
| The enigma machine | A series of electro-mechanical rotor cipher machines, used until the mid 20th century to protect commercial, diplomatic and military communication |
| Entropy (als concept gebruik bij cryptography) | The measure of uncertainty associated with a random variable (must be supplied by the cypher for injection into the plaintext of a message to neutralize an amount of structure) |
| Confusion (als concept gebruik bij cryptography) | Each binary digit of the ciphertext should depend on several parts of the key, thus obscuring the connection between the two. |
| Diffusion (als concept gebruik bij cryptography) | When changing a single bit of plaintext, half of the bits of the ciphertext should also change (approximately) |
| Session Key | Encryption/decryption key that is randomly generated to ensure security of communications between a user and a pc, or between 2 pc’s |
| Ephemeral Key | Not specific, but short lived within a key establishment protocol |

4.2: Identificeer Het Algoritme

Inleiding: Bij deze opdracht heb ik gebruik gemaakt van de online tool [https://www.dcode.fr](https://www.dcode.fr/). Deze tool heeft mij geholpen de cipher texten te decrypteren.

1)

Plaintext: NEVERTRUSTINSECURITYBYOBSCURITY

Ciphertext: ARIREGEHFGVAFRPHEVGLOLBOFPHEVGL

Hier werd er +13 gedaan bij de letters van het alfabet om tot de ciphertext te bekomen, het is van het type shift cipher beter, beter gezegd Caesar cipher. Ook wel bekend als ROT13.

2)

Plaintext: THISISASECRETMESSAGE

Ciphertext: GSRHRHZHVXIVGNVHHZTV

Hier werd er gebruikt gemaakt van de Atbash Cipher, het is een vorm van de Substitution Cipher die vergelijkbaar is met een Caesar cipher. Bij de Atbash Cipher word het alfabet gewoon omgedraaid, de A wordt de Z, de B word de Y enzovoort.

3)

Plaintext: GOOD

Ciphertext: OVUA

Hier werd het woord GOOD geëncrypteerd via de cipher methode vegin

ère. Er werd gebruikt gemaakt van de key “IHGX”. Ik ben hier achter gekomen omdat de “OO” in “GOOD” hetzelfde is, maar in de cipher text “OVUA” is de “V” en de “U” verschillend.

Hierdoor kon het geen shift cipher noch een substitution cipher zijn. En dan bij principe van eliminatie blijft er maar 1 over; de Veginère Cipher.

4.3: Encryptie Conversies

# **Normal:**

There once was a old lass called belle.

She said, "See the lovely repel!"

It was fashionable,

But not unfashionable,

She couldn't say no to the nutshell.

**Ciphertext:**

aolyl vujl dhz h vsk shzz jhsslk ilssl.

zol zhpk, "zll aol svclsf ylwls!"

pa dhz mhzopvuhisl,

iba uva bumhzopvuhisl,

zol jvbsku'a zhf uv av aol ubazolss.

**Base64:**

VGhlcmUgb25jZSB3YXMgYSBvbGQgbGFzcyBjYWxsZWQgYmVsbGUuClNoZSBzYWlkLCAiU2VlIHRoZSBsb3ZlbHkgcmVwZWwhIgpJdCB3YXMgZmFzaGlvbmFibGUsCkJ1dCBub3QgdW5mYXNoaW9uYWJsZSwKU2hlIGNvdWxkbid0IHNheSBubyB0byB0aGUgbnV0c2hlbGwuCg==

**Hex:**

54 68 65 72 65 20 6f 6e 63 65 20 77 61 73 20 61 20 6f 6c 64 20 6c 61 73 73 20 63 61 6c 6c 65 64 20 62 65 6c 6c 65 2e 0a 53 68 65 20 73 61 69 64 2c 20 22 53 65 65 20 74 68 65 20 6c 6f 76 65 6c 79 20 72 65 70 65 6c 21 22 0a 49 74 20 77 61 73 20 66 61 73 68 69 6f 6e 61 62 6c 65 2c 0a 42 75 74 20 6e 6f 74 20 75 6e 66 61 73 68 69 6f 6e 61 62 6c 65 2c 0a 53 68 65 20 63 6f 75 6c 64 6e 27 74 20 73 61 79 20 6e 6f 20 74 6f 20 74 68 65 20 6e 75 74 73 68 65 6c 6c 2e 0a

**Rot13:**

Gurer bapr jnf n byq ynff pnyyrq oryyr.

Fur fnvq, "Frr gur ybiryl ercry!"

Vg jnf snfuvbanoyr,

Ohg abg hasnfuvbanoyr,

Fur pbhyqa'g fnl ab gb gur ahgfuryy.

**AES:**

Atz3hA2heDa38ykI+wxn5SBiz2Ske2yN8kH8xuT6/UYcfMFG/7XnZfB/lzeu3h+MgaCpN2IkR5brea+cCP5JoHA6R+OopmV7YRv2ECbu3k0V9PgKvPr46cP9GLxJoKz8HPO7SIT324s0KHG/tF3/DQB4xP8zGvcuHLajo+FKnxWDQSuoD5Z05SCLB2EAhyk2WcAJ6h+d1N4aGlXXALr6jg==

Key = Team-02-Security

# **Bcrypt:**

$2a$04$LoddKF/COAim3OJI7kYby.QzdfM4/ziebF9ZAWOHvoN/oRdt22FJC

# **Enigma:**

FPHUX KRJHJ EMXCV SBDRE VZSBK WDGGW MFNGP CMBZT RUMAG CPRJN MVMWB QCDDG OTFFG DBWCI GRZQU EBVXC XPTBN RQSQJ AEVFL KORKB GJHWV LPKSR AFYTB PFY

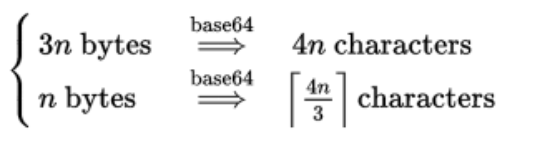
4.4: Verklaring Algoritmes

**Base64**

-zwak, base64 is geen encryptie, maar een encoding.

-geen encryptie

-Heel snel

-Output size: 

-Wordt gebruikt als je binary data wilt overbrengen over een netwerk.

**Hex**

-zwak, hex is geen encryptie, maar een encoding

-Heel snel

-Output size: Dubbel van de input

bv: a wordt 61, ab wordt 61 62

-Wordt gebruikt in assembly om memory addresses voor te stellen.

Ook voor heel wat andere low level computer toepassingen. Soms is het makkelijker met data te werken in hex dan in binary.

**ROT13**

-heel zwak

-symmetrisch, dezelfde key wordt gebruikt om te encrypteren als decrypteren.

bv “hallo” wordt dan “unyyb”. Bij elke letter wordt 13 bij opgeteld.

Als we terug willen van “unyyb” naar “hallo” dan moeten we bij elke letter gewoon weer 13 aftellen.

-Security through obscurity: Reden? De key is hier altijd 13. Iedereen kan dit kraken.

Als het om een gewone caesar cipher ging dan was het eigenlijk Kerckhoff’s principle aangezien je dan eerst de key (1, 2, 3, …, 13, …) moest hebben. Uiteraard aangezien er maar 25 rotaties zijn en niet te veel andere varianten is dit ver van veilig on onkraakbaar.

-ouput size is hetzelfde als input size

-wordt veel gebruikt bij beginner challenges bij CTF’s

**AES**

-heel sterk

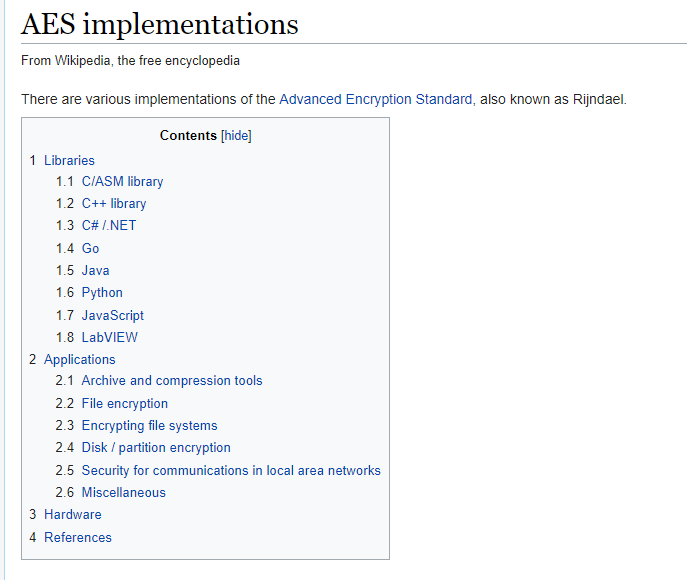
-symmetrisch aangezien dezelfde key gebruikt wordt om te encrypteren als decrypteren.

-kerckhoff’s principle. De key heb je nodig anders ben je er weinig mee. Deze key is 128bits dus is wel zeer moeilijk te kraken.

-heel traag als je geen key hebt, zeer snel als je wel een key hebt.

-Output





Aangezien het een heel sterk algoritme is wordt het ook heel vaak gebruikt.

(zie bovenstaande screenshot)

**Enigma**

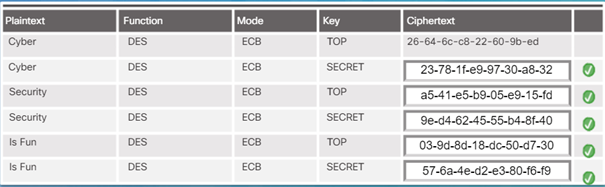
-sterk

-symmetrisch als je de key wist. Hetzelfde algoritme wordt gebruikt om te encrypteren en terug te decrypteren.

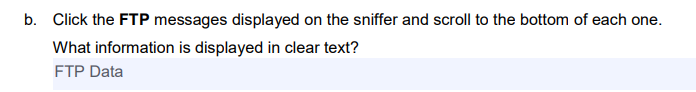
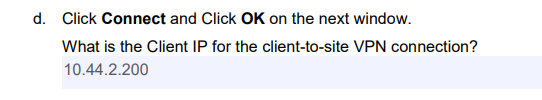
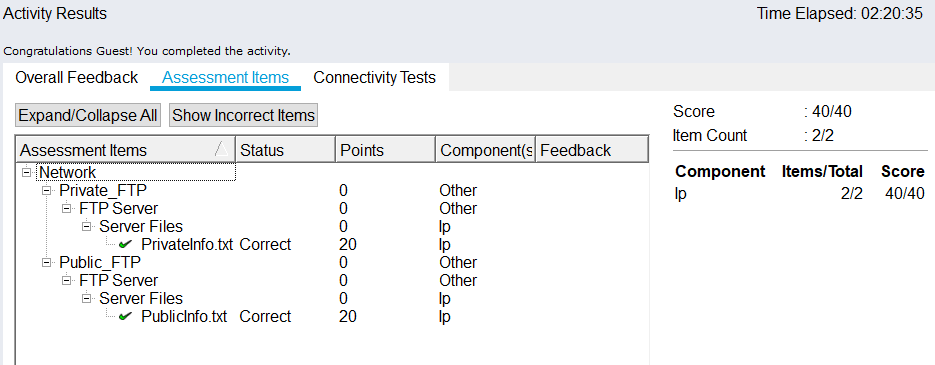
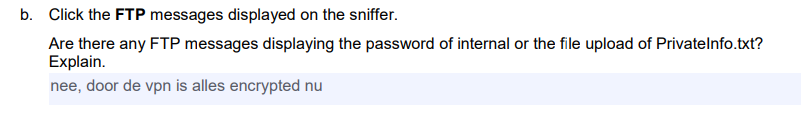
-Kerckhoff’s principle: De britten hadden de machine zelf in eigen hand. Maar aangezien ze de key niet kenden konden ze de berichten nog steeds niet ontmaskeren.

-zeer traag als je geen key hebt, zeer snel als je wel de key hebt.

-Tweede Wereldoorlog

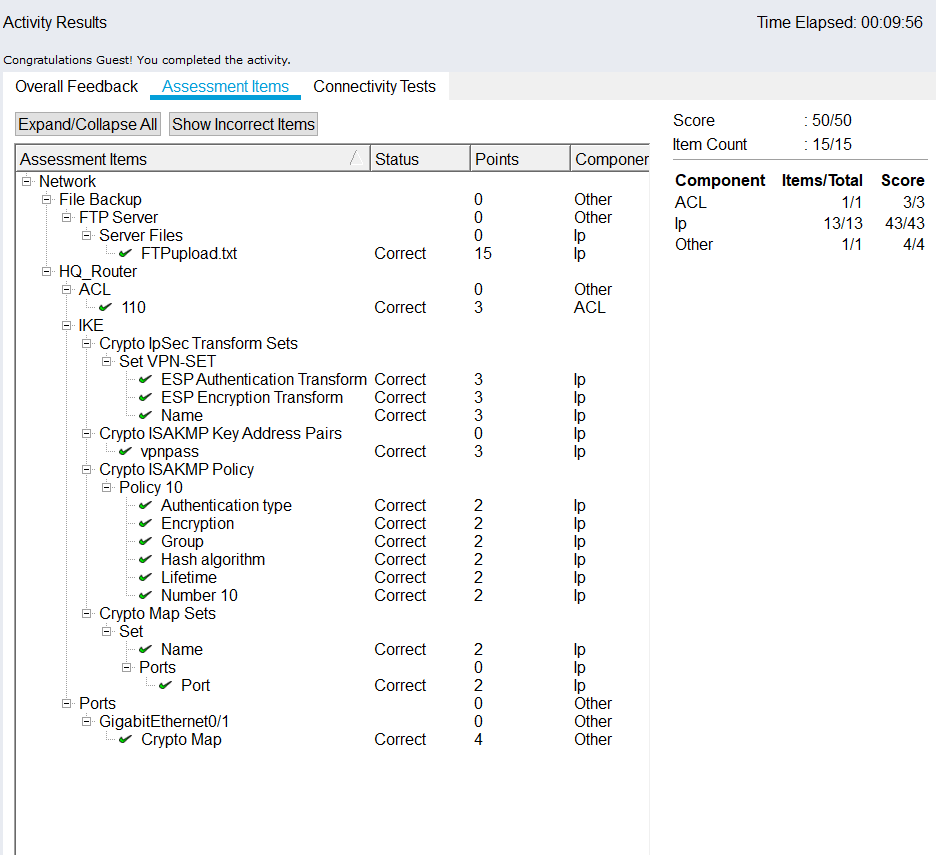
4.5: DES  
  


4.6: Packet Tracer Oefening 4.3.3.3

Note: Het duurde 20min. Mijn klok op Windows stond fout en die had ik terug gezet. blijkbaar heeft dat er twee uur extra bij opgeteld.

4.7: Packet Tracer Oefening



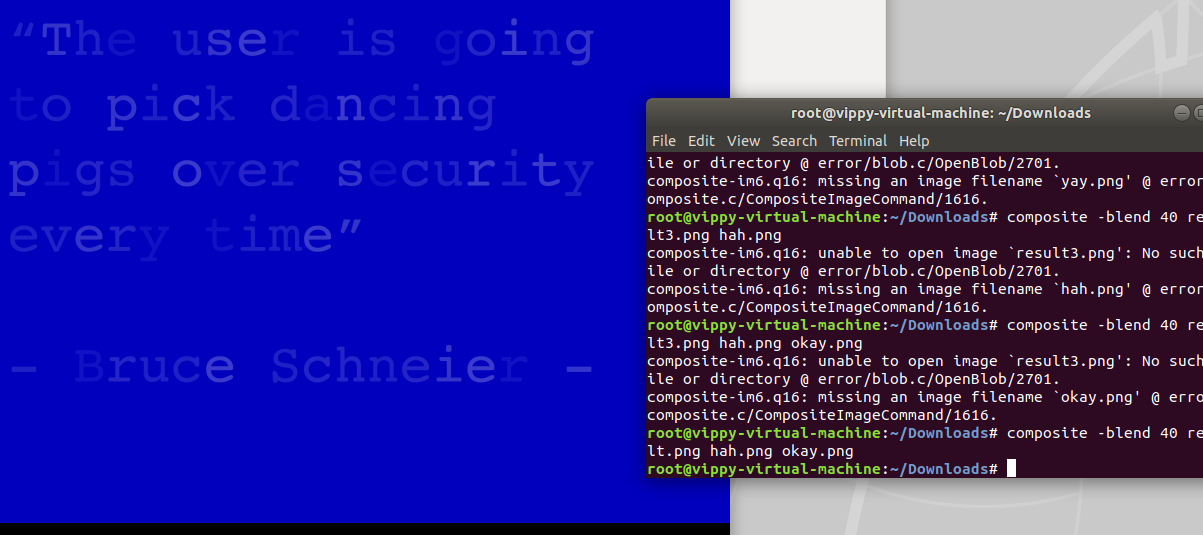
4.8: Crypto Challenges

FLAG LOREMIPSUMDOLORSITAMET (<https://quipqiup.com/> gebruikt)

THEFLAGISNAPIER

HTB{N0T\_A\_Fl1g!}

4.9: File



4.10: Steganography



|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Opdracht | Tijd | Totaal |
| Vicky | 4.8, 4.9, 4.10 Opmaak | 1 uur, 30 min, 30 min 30 min | 2.30 uur |
| Bram | 4.1, 4.3, 4.5 | 1 uur, 15 min, 15 min | 1.30 uur |
| Igor | 4.4, 4.6, 4.7, 4.3 Opmaak + Nakijken | 1 uur, 30 min, 30 min, 15 min, 15 min, 15 min | 2.45 uur |
| Vincent | 4.2 | 45 min | 45 min |

Doorsturen document: Igor