Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

Άσκηση 5
Κρυπτογραφικοί Αλγόριθμοι και Openssl

Αναγνωστόπουλος Άγγελος Νικόλαος
5ο Έτος ΗΜΤΥ
up1066593

5.1.1)
Το openssl έρχεται εγκατεστημένο με την έκδοση debian9 μιας και πολλά από τα πακέτα του debian χρησιμοποιούν τους αλγορίθμους του. Για να ελέγξουμε την έκδοση του, από την κονσόλα του openssl πληκτρολογούμε version. Στην προκειμένη είναι 1.1.0l 10 Sep 2019.

5.1.2)
Με την εντολή openssl ciphers βλέπουμε όλους τους διαθέσιμους αλγορίθμους του openssl για κρυπτογράφιση.

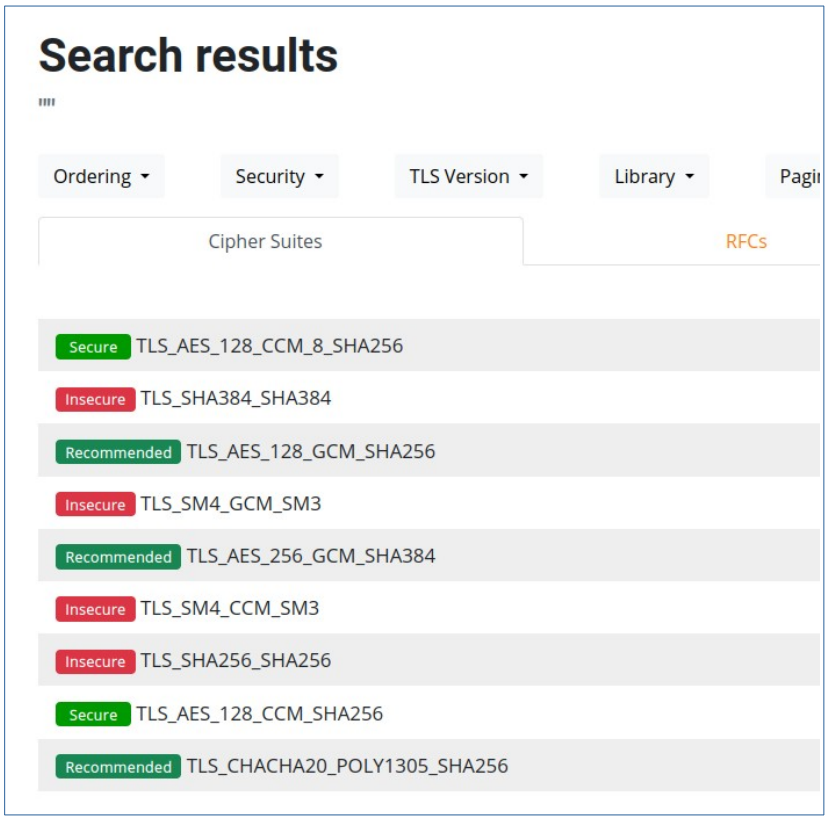
5.1.3)
Για τους αλγορίθμους tls1.3, μπορούμε να χρησιμοποιήσουμε το flag -tls1_3 και να περιορίσουμε σημαντικά τη λίστα στους εξής πέντε αλγορίθμους:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

Φαίνονται με τη σειρά ο αλγόριθμος κρυπτογράφισης, το μέγεθος κλειδιού, ο αλγόριθμος counter mode για τους αλγορίθμους συμμετρικής κρυπτογραφίας και τέλος ο αλγόριθμος hashing και το μέγεθος της αποθηκευμένης (hashed) λέξης.

5.1.4)

Οι αλγόριθμοι που υποστηρίζει το TLS1.3 είναι οι εξής:



5.1.5)

Για τον αλγόριθμο αυτό μπορούμε να δούμε τις λεπτομέρειες του από το ciphersuite. Η δημιουργία κλειδιών με βάση την ελλειπτική κρυπτογραφία είναι ένα τεράστιο κεφάλαιο, αλλά γενικά χρησιμοποιεί ελλειψοειδείς καμπύλες και την κλίση τους σε συγκεκριμένα σημεία, εκμεταλλευόμενη την μαθηματική πολυπλοκότητα των ελλείψεων για να εξασφαλίσει την ίδια ασφάλεια με μικρότερα κλειδιά.

Οι λεπτομέρειες του ECDHE-ECDSA-AES128-GCM-SHA256 είναι οι εξής:

Recommended Cipher Suite

IANA name:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

OpenSSL name:

ECDHE-ECDSA-AES128-GCM-SHA256

GnuTLS name:

TLS_ECDHE_ECDSA_AES_128_GCM_SHA256

Hex code:

0xC0, 0x2B

TLS Version(s):

TLS1.2

Protocol:

Transport Layer Security (TLS)

Key Exchange:

Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)

Authentication:

Elliptic Curve Digital Signature Algorithm (ECDSA)

Encryption:

AEAD Advanced Encryption Standard with 128bit key in Galois/Counter mode (AES 128 GCM)

Hash:

Secure Hash Algorithm 256 (SHA256)

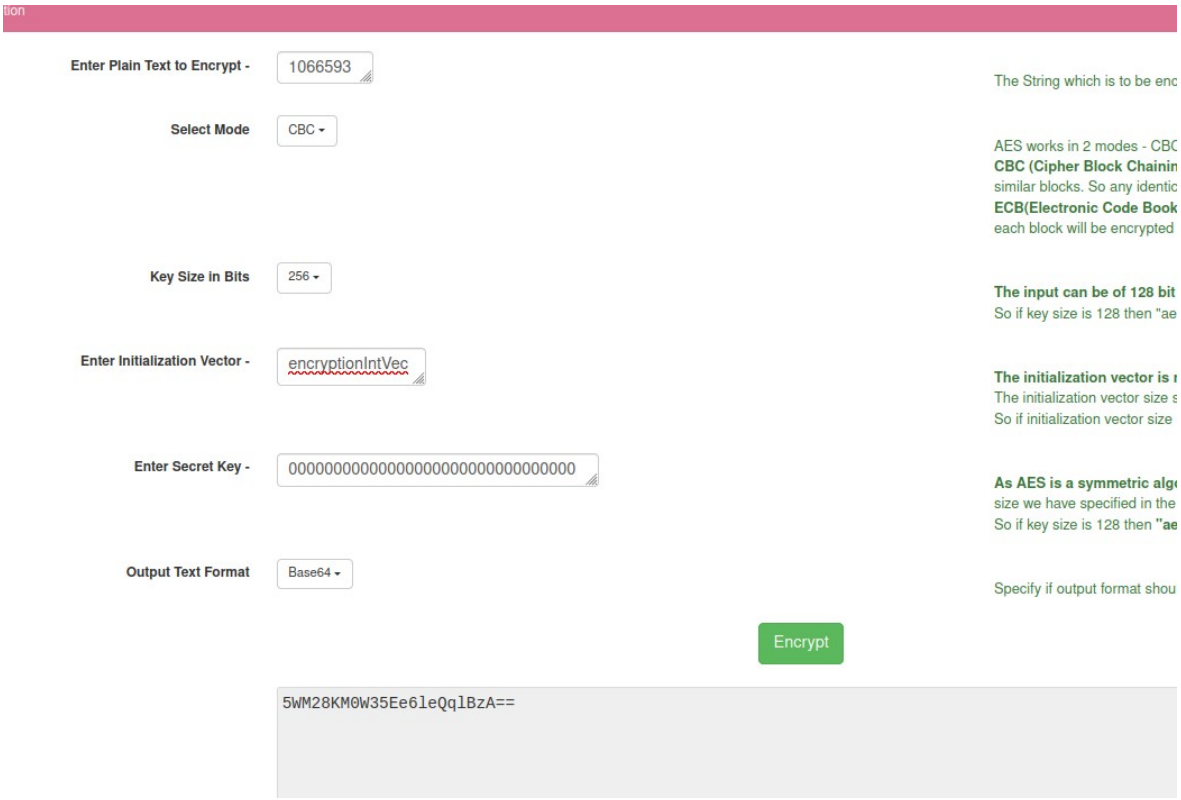
Included in RFC:

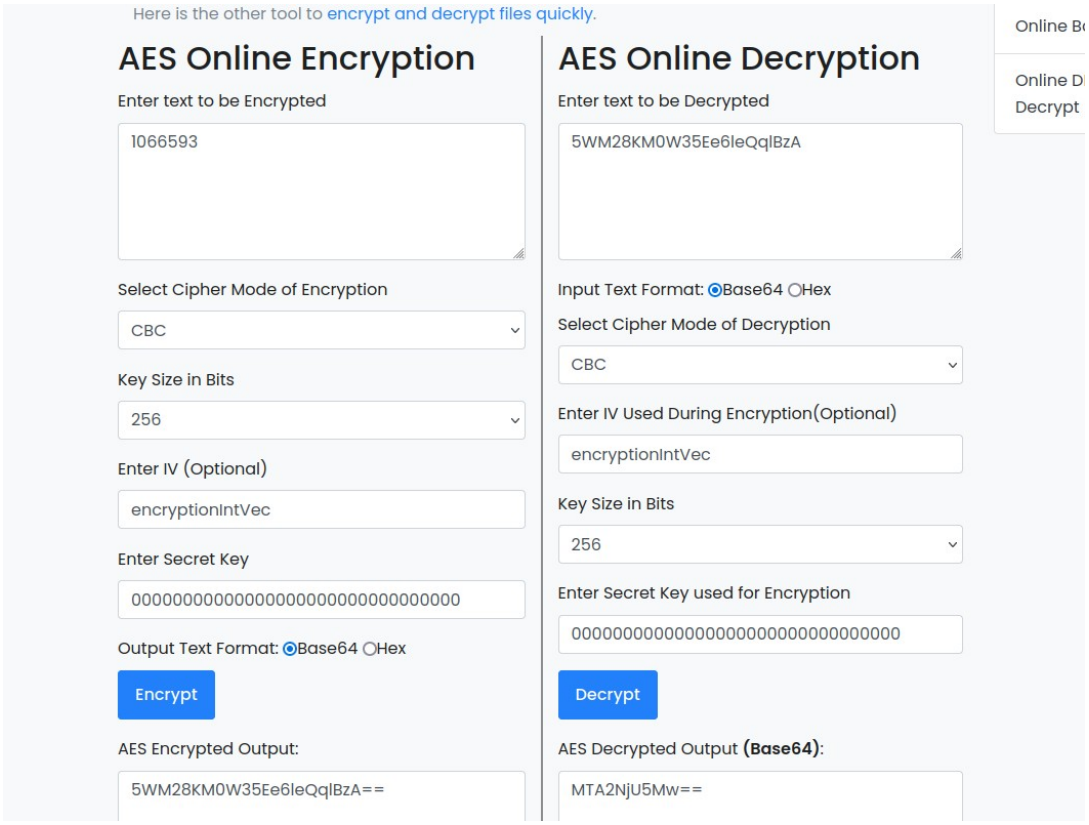
RFC 5289

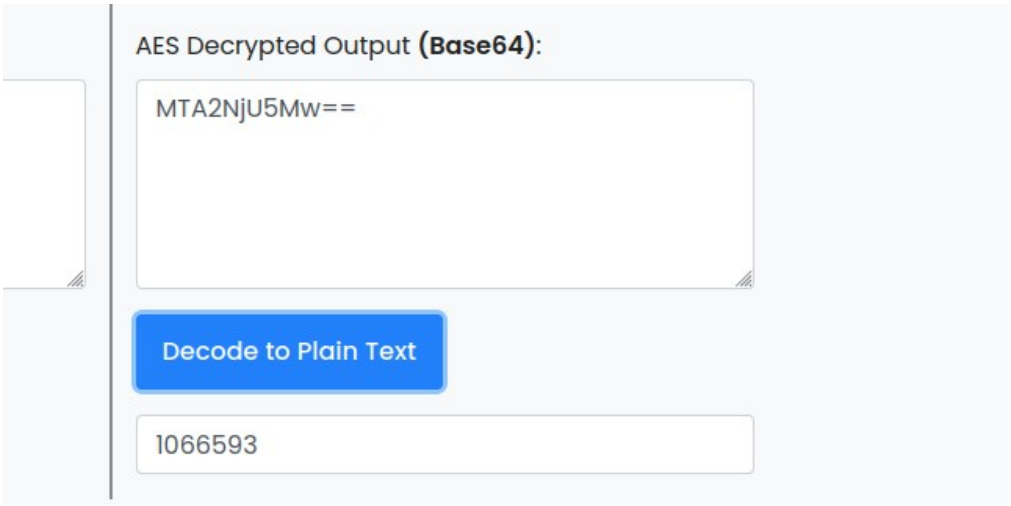
Machine-readable:

application/json

5.1.6)


Enter Plain Text to Encrypt -
1066593
The String which is to be enc
Select Mode
CBC
AES works in 2 modes - CBC
CBC (Cipher Block Chainin
similar blocks. So any identic
ECB(Electronic Code Book
each block will be encrypted
Key Size in Bits
256
The input can be of 128 bit
So if key size is 128 then "ae
Enter Initialization Vector -
encryptionIntVec
The initialization vector is
The initialization vector size
So if initialization vector size
Enter Secret Key -
00000000000000000000000000000000
As AES is a symmetric alg
size we have specified in the
So if key size is 128 then "ae
Output Text Format
Base64
Specify if output format shou
Encrypt
5WM28KM0W35Ee6leQqlBzA==


Here is the other tool to encrypt and decrypt files quickly.
AES Online Encryption
Enter text to be Encrypted
1066593
Select Cipher Mode of Encryption
CBC
Key Size in Bits
256
Enter IV (Optional)
encryptionIntVec
Enter Secret Key
00000000000000000000000000000000
Output Text Format: Base64 Hex
Encrypt
AES Encrypted Output:
5WM28KM0W35Ee6leQqlBzA==
AES Online Decryption
Enter text to be Decrypted
5WM28KM0W35Ee6leQqlBzA
Input Text Format: Base64 Hex
Select Cipher Mode of Decryption
CBC
Enter IV Used During Encryption(Optional)
encryptionIntVec
Key Size in Bits
256
Enter Secret Key used for Encryption
00000000000000000000000000000000
Decrypt
AES Decrypted Output (Base64):
MTA2NjU5Mw==
Online B
Online D
Decrypt



5.1.7)

Τα hashing functions είναι μέθοδοι που επιδρούν επάνω σε μία είσοδο και την μετασχηματίζουν με κάποιο τρόπο σε μία έξοδο. Αυτή η έξοδος πρέπει να είναι ενός σταθερού μήκους άσχετα με το μέγεθος της εισόδου, να μην υπάρχουν (πολλά) duplications εξόδου για διαφορετικές εισόδους (Δηλ. If A != B => Hash(A) != Hash(B) for all A,B) και τέλος η διαδικασία να γίνεται γρήγορα άσχετα με το μέγεθος της εισόδου. Η διαδικασία αυτή είναι μονόπλευρη (σε αντίθεση με την κρυπτογράφιση) και ο μόνος τρόπος να ελεγχθεί ένα hash είναι να βρούμε με κάποιο τρόπο την είσοδο που το δημιουργεί. Η πιο απλή (και όχι πολύ καλή με βάση τα standards μας) hashing function είναι να χωρίσουμε την είσοδο μας σε j blocks και να κάνουμε ένα απλό bitwise XOR για κάθε i-th bit και j-th block.