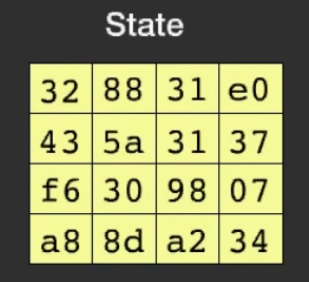
**Ανάλυση αλγορίθμου κρυπτογράφησης AES**

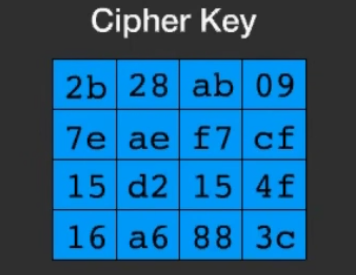
Το όνομα αυτού νου του αλγορίθμου βγαίνει από τις λέξεις Advanced Encryption Standard. Το εναλλακτικό του όνομα είναι Rijndael και δημιουργήθηκε από δύο Βέλγους κρυπτογράφους το 2001. Χρησιμοποιήθηκε στην αρχή από την αμερικάνικη κυβέρνηση και τώρα χρησιμοποιείται διεθνώς από πολλούς οργανισμούς. Δημιουργήθηκε για να αντικαταστήσει έναν άλλο αλγόριθμο κρυπτογράφησης εν ονόματι Data Encryption Standard (DES), ο οποίος δημοσιοποιήθηκε το 1977. Ο AES αποτελεί έναν συμμετρικό αλγόριθμο κρυπτογράφησης, δηλαδή χρησιμοποιεί το ίδιο κλειδί για να κρυπτογραφήσει και να αποκρυπτογραφήσει δεδομένα. Αποτελεί έναν πολύ ασφαλές αλγόριθμό κρυπτογράφησης αφού είναι ο πρώτος και ο μοναδικός που έχει εγκριθεί από την National Security Agency (NSA) για την ασφάλεια των δεδομένων της.

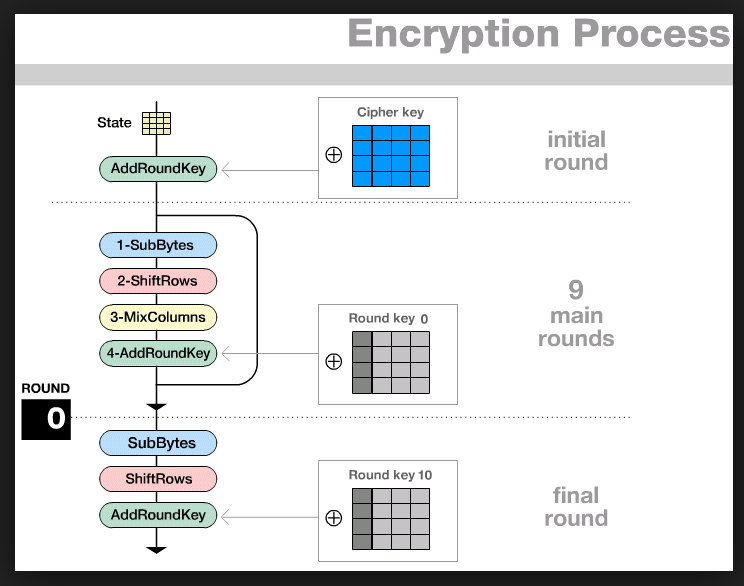
Ο αλγόριθμος αυτός χρειάζεται όπως τους άλλους συνηθισμένου αλγορίθμους κρυπτογράφησης ένα κείμενο (Plain text) καθώς και ένα κλειδί(Cypher Key) καθώς με την χρήση του κλειδιού αυτού θα γίνει η κρυπτογράφηση του κειμένου.

Ο παρακάτω αλγόριθμος χρησιμοποιεί κρυπτογράφηση ανά block, καθώς κρυπτογραφεί 16 bits την φορά όπως βλέπουμε παρακάτω:



Και το κλειδί θα είναι διαιρεμένο σε 16 bits την φορά:



Διαδικασία:

Όπως βλέπουμε και στην εικόνα, ο αλγόριθμος AES για την κρυπτογράφηση του μηνύματος εκτελεί τις ακόλουθες συναρτήσεις:

* AddRoundKey
* SubBytes
* MixColumns
* AddRoundkey

Υπάρχουν 3 είδη κατηγοριών που μπορεί να έχουμε σε αυτόν τον αλγόριθμο.

Να είναι το κείμενο (Plain Text):

1. 128 bits
2. 192 bits
3. 256 bits

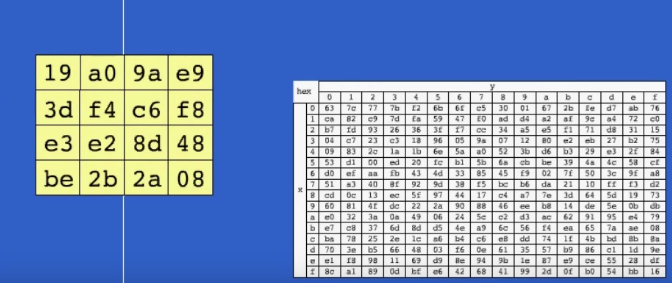
Για τις παραπάνω κατηγορίες οι αριθμοί των γύρων που βλέπουμε στην παραπάνω εικόνα αλλάζει.

Δηλαδή αν έχουμε 128 bits τότε θα γίνουν 10 επαναλήψεις , αν έχουμε 192 θα γίνουν 12 και αν έχουμε 256 θα γίνουν 14. Δηλαδή ο αριθμός εκτέλεσης των παραπάνω συναρτήσεων φαίνεται στον πίνακα:

|  |  |  |  |
| --- | --- | --- | --- |
| Αριθμός Bits: | 128 | 192 | 256 |
| AddRoundKey | 12 | 14 | 16 |
| SubBytes | 11 | 13 | 15 |
| MixColumns | 10 | 12 | 14 |
| ShiftRows | 11 | 13 | 15 |

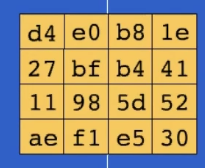
**Ανάλυση συναρτήσεων:**

1. SubBytes:



Καθώς έχουμε το παραπάνω block ή αλλιώς state, παίρνουμε και αντικαθιστούμε το κάθε bit με την τιμή που έχει στον άσπρο πίνακα που λέγεται S-BOX. Αυτό το κάνουμε σε όλα τα bits του block.

Στο τέλος θα γίνει σύμφωνα με τον πίνακα έτσι:



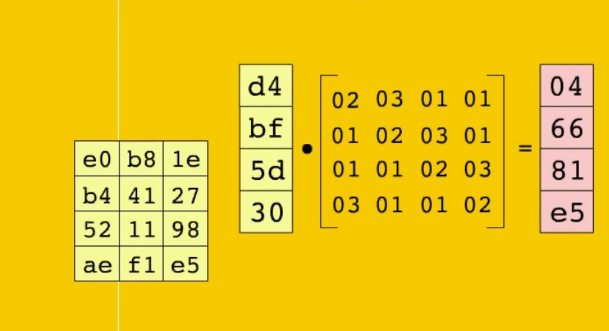
1. ShiftRows:

Στην συγκεκριμένη διαδικασία παίρνουμε την δεύτερη σειρά του block και την κάνουμε rotate κατά ένα byte. Στην Τρίτη σειρά θα την κάνουμε rotate ανά 2 byte ενώ στο τελευταία σειρά θα την κάνουμε rotate ανά 3 byte και θα γίνει κάπως έτσι:

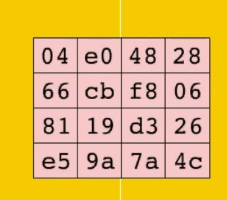


1. MixColumns:

Σε αυτήν την διαδικασία παίρνουμε την πρώτη στήλη του block και την πολλαπλασιάζουμε με έναν συγκεκριμένο πίνακα όπως φαίνεται και στην εικόνα:



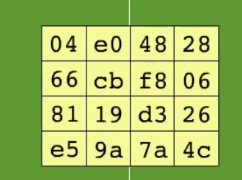
Συνεχίζουμε και με τις άλλες στήλες, ώστε το αποτέλεσμα να είναι κάπως έτσι:



1. AddRoundkey

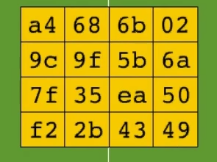
Σε αυτήν την συνάρτηση παίρνουμε το παραγόμενο κλειδί (θα δείξουμε μετά πως υπολογίζεται) και το προσθέτουμε στο state που έχουμε.

Πχ . Έστω το state που είχαμε υπολογίσαμε πιο πριν:



Και το παραγόμενο κλειδί (Round Key):

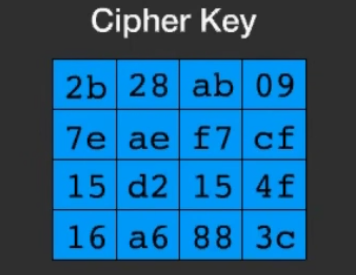
Μετά την πρόσθεση θα γίνει έτσι το state μας:



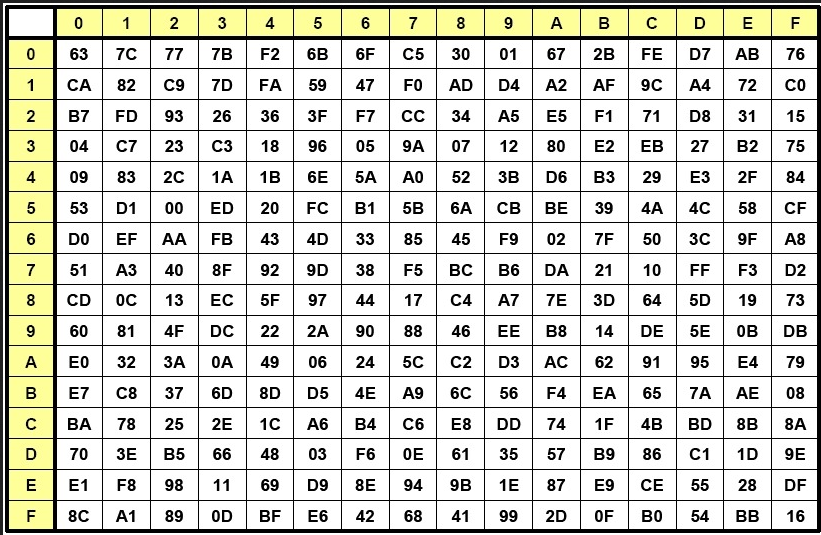
1. Υπολογισμός παραγόμενου κλειδιού

Για την παραγωγή κλειδιών θα χρησιμοποιήσουμε το αρχικό κλειδί που δίνει ο χρήστης καθώς τους πίνακες S-BOX και Rcon που είναι τα παρακάτω:

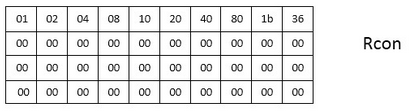
Αρχικό κλειδί που εισάγαμε:



S-BOX:



Rcon:



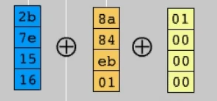
Πρώτον, παίρνουμε την τελευταία στήλη του cypher key μας, κάνουμε ένα rotate προς τα πάνω ώστε να γίνει έτσι:



Δεύτερον, αντικαθιστούμε τα bits που έχουμε , με τα bits του πίνακα S-BOX ώστε να γίνει έτσι:



Τρίτον, προσθέτουμε την πρώτη στήλη του cypher key με την στήλη που παράξαμε στο 2ο βήμα καθώς με την 1 στήλη του πίνακα Rcon, δηλαδή όπως φαίνεται παρακάτω:



Η πρόσθεση αυτή θα μας βγάλει την πρώτη στήλη του νέου round key.



Για να βγάλουμε τις άλλες στήλες θα πρέπει να προσθέσουμε την παραπάνω στήλη που παράξαμε με τις αντίστοιχες 2η, 3η και 4η στήλη του αρχικού cypher key και το αποτέλεσμα που θα μας βγάλει θα είναι το παρακάτω:

Νέο round Key:



Για να φτιάξουμε το 2ο round key ακολουθεί η ίδια περίπου διαδικασία , καθώς οι διαφορές που συναντάμε είναι ότι αντί να πάρουμε το block του cypher key που έβγαλε ο χρήστης, θα πάρουμε το νέο round key που παράξαμε καθώς και θα προσθέσουμε σε αυτό όχι την 1η στήλη του Rcon αλλά την 2η .