

AES

AES (англ. Advanced Encryption Standard) – вариант на симетричен блок шифър на Rijndael.

AES

AES (англ. Advanced Encryption Standard) – вариант на симетричен блок шифър на Rijndael.

Избран от правителството на САЩ за защита на класифицирана информация.

AES

AES (англ. Advanced Encryption Standard) – вариант на симетричен блок шифър на Rijndael.

Избран от правителството на САЩ за защита на класифицирана информация.

Националният институт за стандарти и технологии (NIST) е започнал разработването на AES през 1997 г., като заместител на стандарта за шифроване на данни DES (англ. Data Encryption Standard), който е станал уязвим на brute-force атаки.

www.euroqci.bg

- Като всеки симетричен шифър, AES използва един и същ ключ за криптиране и декриптиране на данните.

- Като всеки симетричен шифър, AES използва един и същ ключ за криптиране и декриптиране на данните.
- Ефективен както по отношение на софтуерна, така и по отношение на хардуерна имплементация.

- Като всеки симетричен шифър, AES използва един и същ ключ за криптиране и декриптиране на данните.
- Ефективен както по отношение на софтуерна, така и по отношение на хардуерна имплементация.
- Алгоритъмът работи с редици от 16 байта, записани като 4x4 матрици, като използва определен брой кръгове от трансформации (round function) върху тези матрици.

- Размерът на ключа (128, 192 или 256 бита) определя броя на кръговете от трансформации, които преобразуват входа. AES с 256 битов ключ използва 14 кръга.

- Размерът на ключа (128, 192 или 256 бита) определя броя на кръговете от трансформации, които преобразуват входа. AES с 256 битов ключ използва 14 кръга.
- Този ключ е инициращ, и чрез конкретен алгоритъм от него се извеждат 128 битови ключове - по един за всеки кръг от трансформации

- Повечето от изчисленията се правят в крайното поле

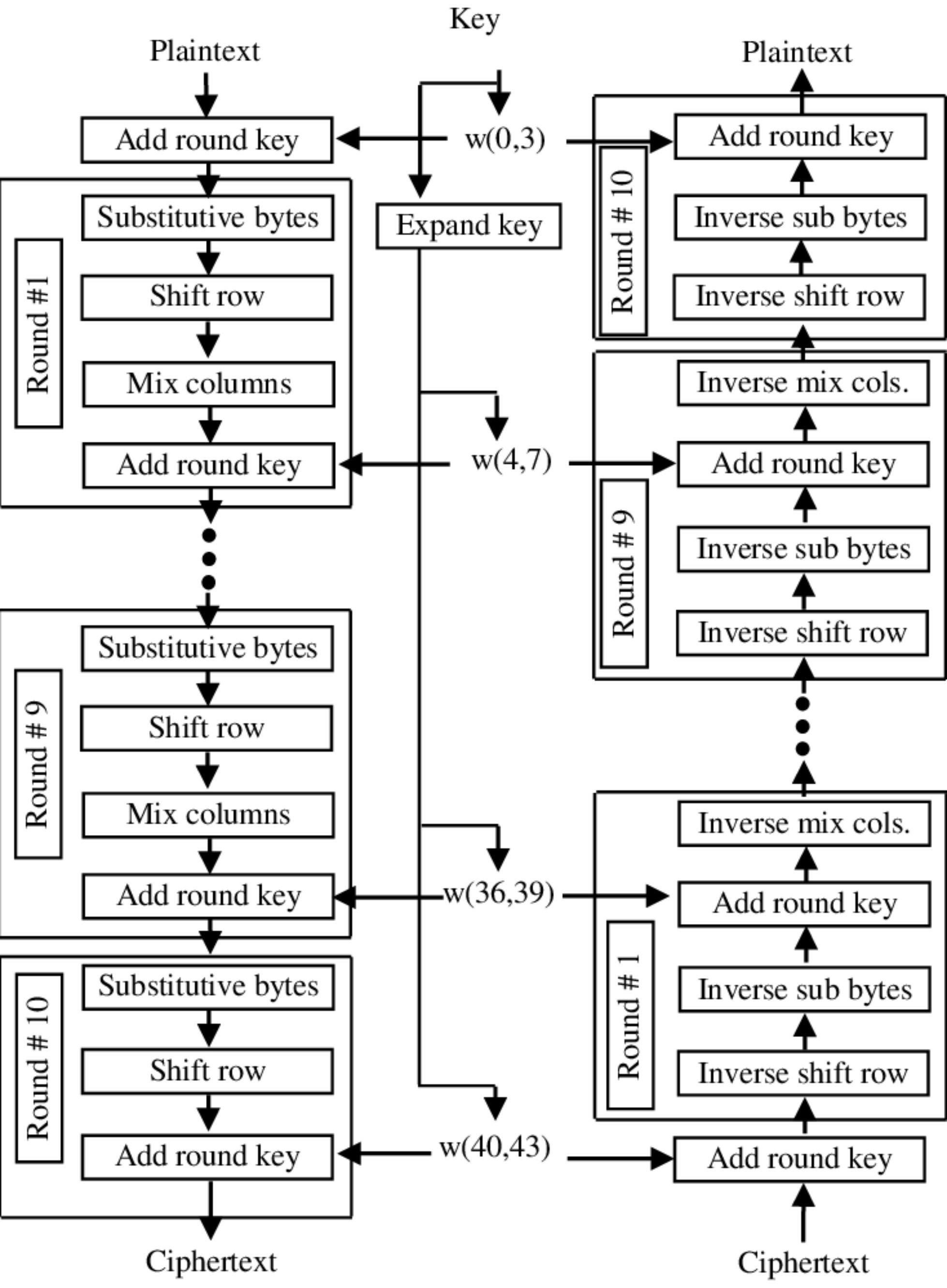
$$GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1),$$

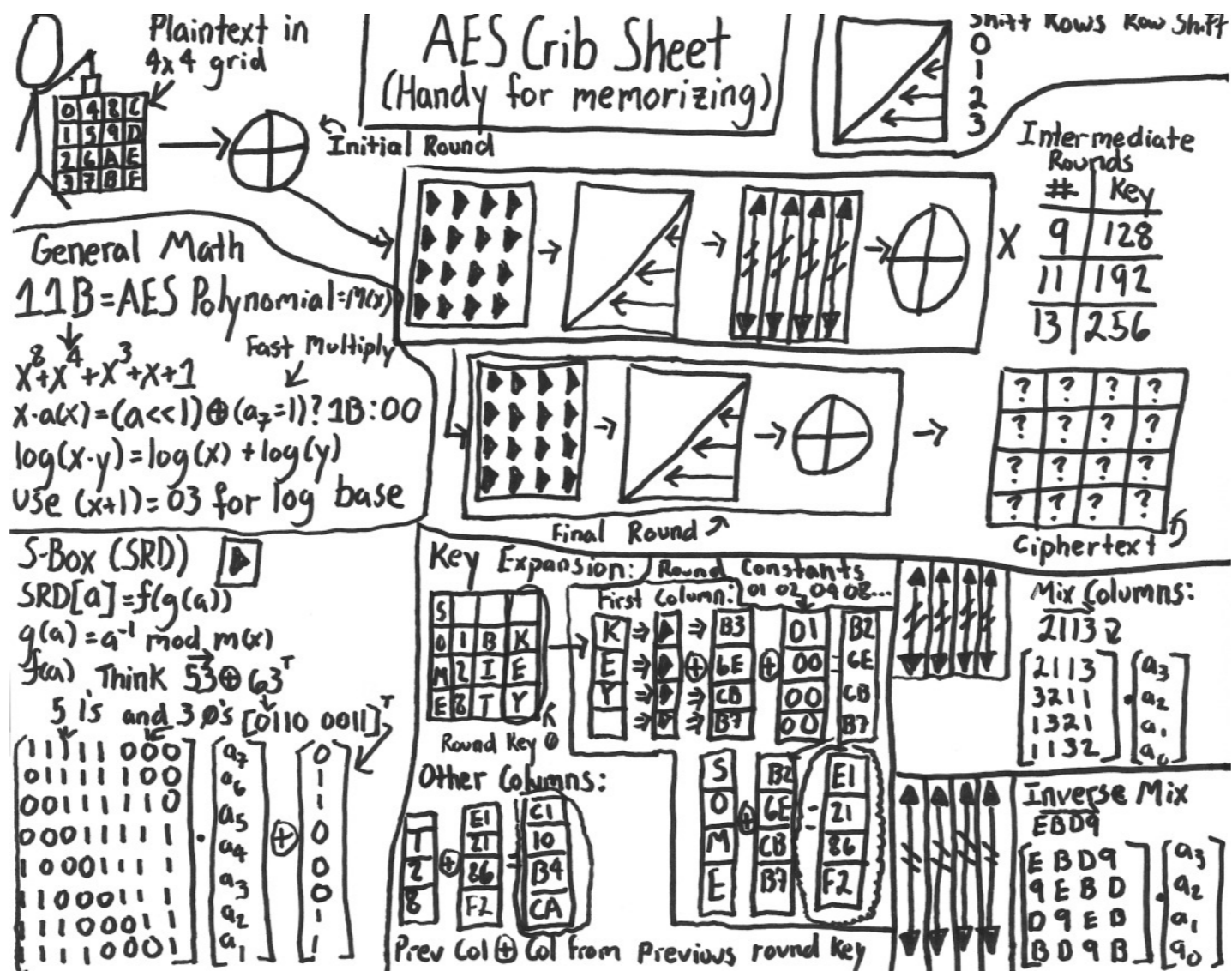
където $GF(2)$ е полето с два елемента, 0 и 1,

със събиране и умножение по модул 2 като полеви операции.

- Всички кръгове, с изключение на последния, се състоят от 4 стъпки:
 - заместване на елементите на матрицата с помощта на S-кутия на Rijndael,
 - (циклични) пермутации на елементите в редовете на матрицата,
 - смесване на елементите от дадена колона (посредством матрично умножение с предварително зададена матрица),
 - добавяне на 128 битов ключ

- Заместването се извършва с помощта на S-кутия на Rijndael, базирана на нелинейна операция, която е заместване на елемент от крайното поле $GF(2^8)$ с неговият мултипликативен обратен елемент и последваща афийна трансформация.





- Вариантите на AES работещи с размери на ключове под 128 бита ще бъдат компрометирани от квантовия алгоритъм за търсене на Гроувър, който осигурява по-бързо търсене през всички възможни ключове за дешифриране на криптираното съобщение.

- Вариантите на AES работещи с размери на ключове под 128 бита ще бъдат компрометирани от квантовия алгоритъм за търсене на Гроувър, който осигурява по-бързо търсене през всички възможни ключове за дешифриране на криптираното съобщение.
- Тази заплаха може да бъде предотвратена чрез увеличаване на дължината на ключа до 256 бита, което прави времето за търсене непрактично дълго дори за квантов компютър. Това твърдение е в сила при предположение, че не съществува квантова атака, по-ефективна от алгоритъма на Гроувър, което не е доказано.

- Тъй като AES използва симетричен ключ, за да обменят този ключ, комуникиращите страни следват протокол за обмен на ключове, напр. удостоверяване чрез TLS (англ. Transport Layer Security).

Тъй като AES използва симетричен ключ, за да обменят този ключ, комуникиращите страни следват протокол за обмен на ключове, напр. удостоверяване чрез TLS (англ. Transport Layer Security). Този процес използва асиметрична двойка ключове, състояща се от математически свързани частен и публичен ключ. Едната страна „подписва“ предаваната информация с частен ключ, докато другата страна математически проверява подписа с помощта на публичния ключ.

Тъй като AES използва симетричен ключ, за да обменят този ключ, комуникиращите страни следват протокол за обмен на ключове, напр. удостоверяване чрез TLS (англ. Transport Layer Security). Този процес използва асиметрична двойка ключове, състояща се от математически свързани частен и публичен ключ. Едната страна „подписва“ предаваната информация с частен ключ, докато другата страна математически проверява подписа с помощта на публичния ключ. Сигурността се основава на трудността при решаване на математически проблеми, напр. в RSA протокола това е факторизиране на число, което е произведение на две големи прости числа.

QKD е подходящо решение за генериране и обмен на ключове за AES 256 по сигурен начин. Избрахме тази комбинация, от QKD и AES 256, при за изграждането на първата QKD мрежа в България, която е част от Европейската квантово-комуникационна инфраструктура.

QKD е подходящо решение за генериране и обмен на ключове за AES 256 по сигурен начин. Избрахме тази комбинация, от QKD и AES 256, при за изграждането на първата QKD мрежа в България, която е част от Европейската квантово-комуникационна инфраструктура.

Практическата цел на интегрирането на QKD платформи с криптори AES256 е да се гарантира, че ключовете, разпространявани от QKD системите, се използват по сигурен начин.

