Lab final project report

ELCE 202

Team members:

Sanzhar Yergaliyev, Id: 201894694

Abzal Aidakhmetov, Id: 201726640

Rauan Toilybayev, Id: 201740372

Date: 05.12.20

Contribution

Sanzhar

Module names: Key expansion, (inverse) Mix columns, Encryption, Decryption.

Abzal

Module names: (inverse) Shift rows, Test bench.

Rauan

Module names: (inverse) Byte substitution.

Peripherral work: Report

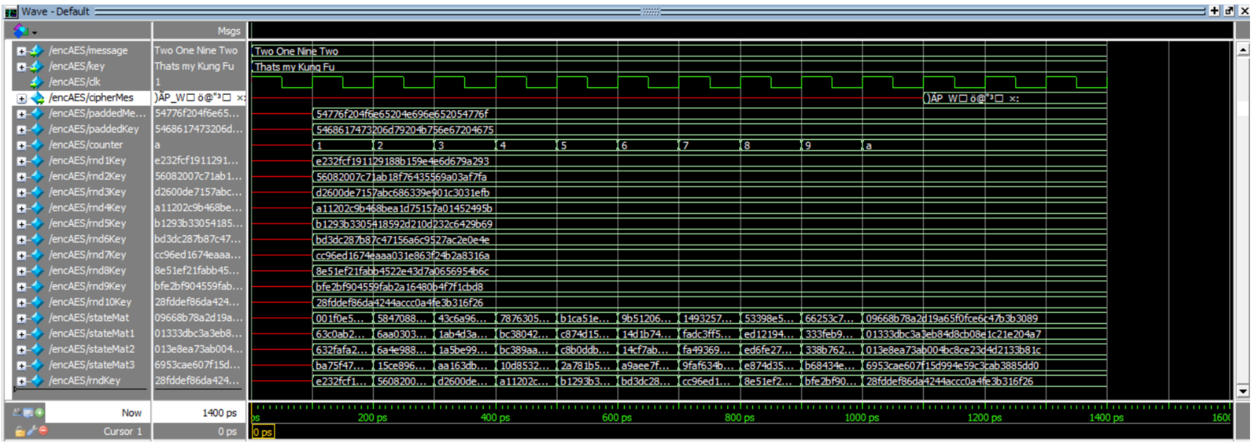
Implemented protion of project

Every part of 128 bit encryption and decryption is implemented.

But we lack a block wise divider logic that allows to input larger than 128 bit messages and cipher texts. So the input is bounded by 128 bits.

Screen shots of simulation

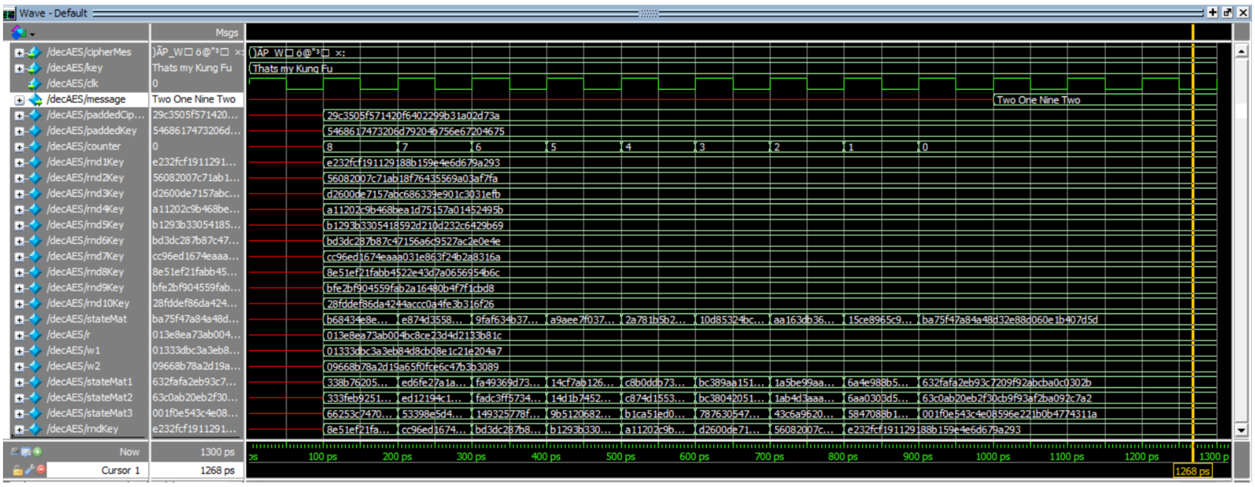
Simulation of encryption of the provided example:



```
/encAES/message      Two One Nine Two       Two One Nine Two
/encAES/key          Thats my Kung Fu       Thats my Kung Fu
/encAES/clk          1
/encAES/cipherMes    )ÄP_W□ ö@"³□ ×:        )ÄP W□ ö@"³□ ×:
/encAES/paddedMe...  54776f204f6e65...      54776f204f6e65204e696e652054776f
/encAES/paddedKey    5468617473206d...      5468617473206d79204b756e67204675
/encAES/counter      a                      1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a
/encAES/rnd1Key      e232fcf1911291...      e232fcf191129188b159e4e6d679a293
/encAES/rnd2Key      56082007c71ab1...      56082007c71ab18f76435569a03af7fa
/encAES/rnd3Key      d2600de7157abc...      d2600de7157abc686339e901c3031efb
/encAES/rnd4Key      a11202c9b468be...      a11202c9b468bea1d75157a01452495b
/encAES/rnd5Key      b1293b33054185...      b1293b3305418592d210d232c6429b69
/encAES/rnd6Key      bd3dc287b87c47...      bd3dc287b87c47156a6c9527ac2e0e4e
/encAES/rnd7Key      cc96ed1674eaaa...      cc96ed1674eaaa031e863f24b2a8316a
/encAES/rnd8Key      8e51ef21fabb45...      8e51ef21fabb4522e43d7a0656954b6c
/encAES/rnd9Key      bfe2bf904559fab...     bfe2bf904559fab2a16480b4f7f1cbd8
/encAES/rnd10Key     28fddef86da424...      28fddef86da4244accc0a4fe3b316f26
/encAES/stateMat     09668b78a2d19a...      001f0e5... | 5847088... | 43c6a96... | 7876305... | b1ca51e... | 9b51206... | 1493257... | 53398e5... | 66253c7... | 09668b78a2d19a65f0fce6c47b3b3089
/encAES/stateMat1    01333dbc3a3eb8...      63c0ab2... | 6aa0303... | 1ab4d3a... | bc38042... | c874d15... | 14d1b74... | fadc3ff5... | ed12194... | 333feb9... | 01333dbc3a3eb84d8cb08e1c21e204a7
/encAES/stateMat2    013e8ea73ab004...      632fafa2... | 6a4e988... | 1a5be99... | bc389aa... | c8b0ddb... | 14cf7ab... | fa49369... | ed6fe27... | 338b762... | 013e8ea73ab004bc8ce23d4d2133b81c
/encAES/stateMat3    6953cae607f15d...      ba75f47... | 15ce896... | aa163db... | 10d8532... | 2a781b5... | a9aee7f... | 9faf634b... | e874d35... | b68434e... | 6953cae607f15d994e59c3cab3885dd0
/encAES/rndKey       28fddef86da424...      e232fcf1... | 5608200... | d2600de... | a11202c... | b1293b3... | bd3dc28... | cc96ed1... | 8e51ef2... | bfe2bf90... | 28fddef86da4244accc0a4fe3b316f26

Now        1400 ps      ps   200 ps   400 ps   600 ps   800 ps   1000 ps   1200 ps   1400 ps   160(
Cursor 1   0 ps         0 ps
```

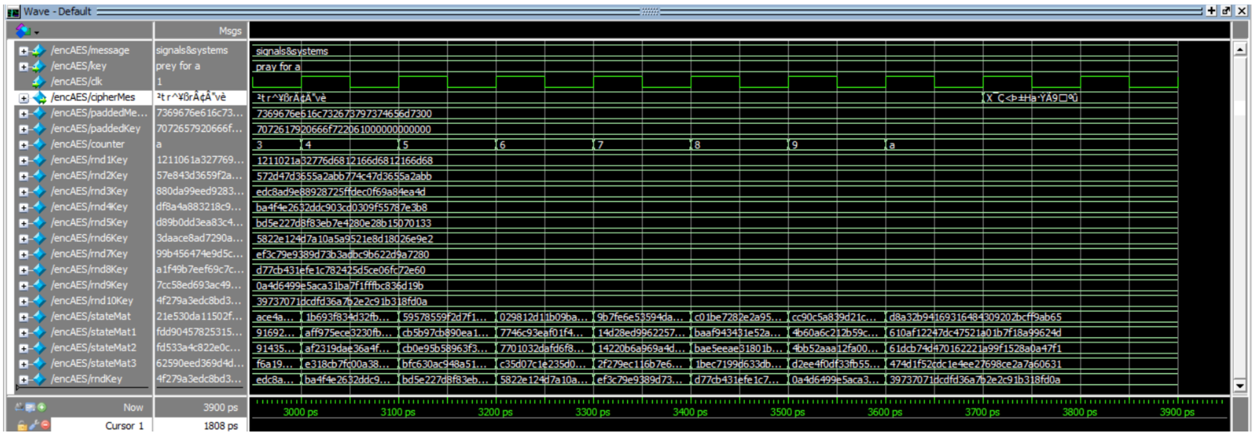
Simulation of decryption of the provided example:



Wave - Default

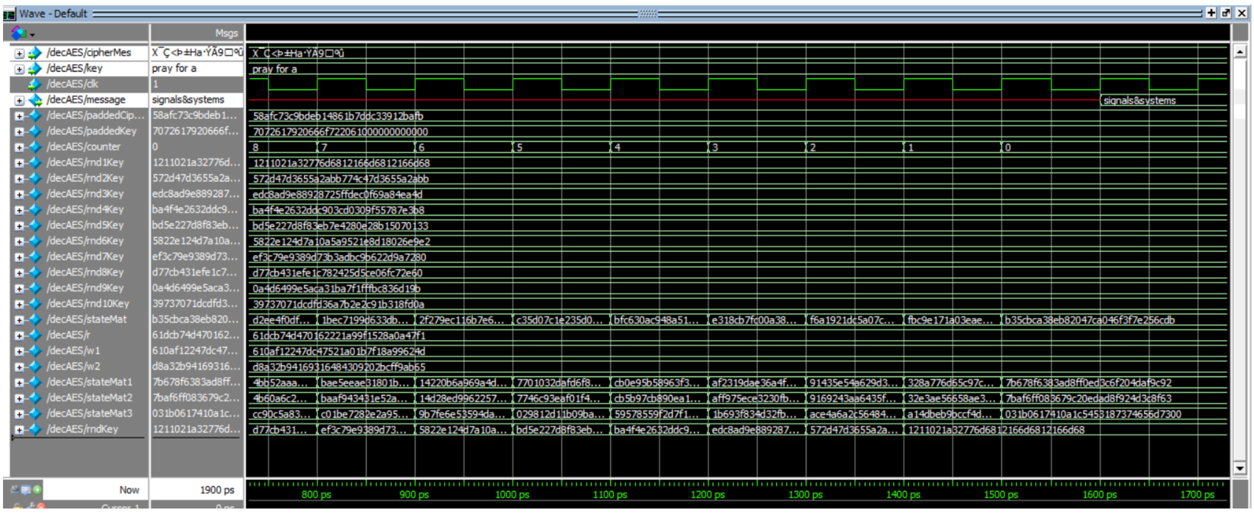
	Msgs
/decAES/cipherMes	)ÃP_W□ ö@"³□ ×:
/decAES/key	Thats my Kung Fu
/decAES/clk	0
/decAES/message	Two One Nine Two
/decAES/paddedCip...	29c3505f571420...
/decAES/paddedKey	5468617473206d...
/decAES/counter	0
/decAES/rnd1Key	e232fcf1911291...
/decAES/rnd2Key	56082007c71ab1...
/decAES/rnd3Key	d2600de7157abc...
/decAES/rnd4Key	a11202c9b468be...
/decAES/rnd5Key	b1293b33054185...
/decAES/rnd6Key	bd3dc287b87c47...
/decAES/rnd7Key	cc96ed1674eaaa...
/decAES/rnd8Key	8e51ef21fabb45...
/decAES/rnd9Key	bfe2bf904559fab...
/decAES/rnd10Key	28fddef86da424...
/decAES/stateMat	ba75f47a84a48d...
/decAES/r	013e8ea73ab004...
/decAES/w1	01333dbc3a3eb8...
/decAES/w2	09668b78a2d19a...
/decAES/stateMat1	632fafa2eb93c7...
/decAES/stateMat2	63c0ab20eb2f30...
/decAES/stateMat3	001f0e543c4e08...
/decAES/rndKey	e232fcf1911291...
Now	1300 ps
Cursor 1	1268 ps

Simulation of encrpytion and decryption of a generic input:



Wave - Default

	Msgs
/encAES/message	signals&systems
/encAES/key	prey for a
/encAES/clk	1
/encAES/cipherMes	²t r^¥ßrÂ¢Â¨vè
/encAES/paddedMe...	7369676e616c73...
/encAES/paddedKey	7072657920666f...
/encAES/counter	a
/encAES/rnd1Key	1211061a327769...
/encAES/rnd2Key	57e843d3659f2a...
/encAES/rnd3Key	880da99eed9283...
/encAES/rnd4Key	df8a4a883218c9...
/encAES/rnd5Key	d89b0dd3ea83c4...
/encAES/rnd6Key	3daace8ad7290a...
/encAES/rnd7Key	99b456474e9d5c...
/encAES/rnd8Key	a1f49b7eef69c7c...
/encAES/rnd9Key	7cc58ed693ac49...
/encAES/rnd10Key	4f279a3edc8bd3...
/encAES/stateMat	21e530da11502f...
/encAES/stateMat1	fdd90457825315...
/encAES/stateMat2	fd533a4c822e0c...
/encAES/stateMat3	62590eed369d4d...
/encAES/rndKey	4f279a3edc8bd3...
Now	3900 ps
Cursor 1	1808 ps



Wave - Default

	Msgs
/decAES/cipherMes	X¯Ç<Þ±Ha·ÝÃ9□ºû
/decAES/key	pray for a
/decAES/clk	1
/decAES/message	signals&systems
/decAES/paddedCip...	58afc73c9bdeb1...
/decAES/paddedKey	7072617920666f...
/decAES/counter	0
/decAES/rnd1Key	1211021a32776d...
/decAES/rnd2Key	572d47d3655a2a...
/decAES/rnd3Key	edc8ad9e889287...
/decAES/rnd4Key	ba4f4e2632ddc9...
/decAES/rnd5Key	bd5e227d8f83eb...
/decAES/rnd6Key	5822e124d7a10a...
/decAES/rnd7Key	ef3c79e9389d73...
/decAES/rnd8Key	d77cb431efe1c7...
/decAES/rnd9Key	0a4d6499e5aca3...
/decAES/rnd10Key	39737071dcdfd3...
/decAES/stateMat	b35cbca38eb820...
/decAES/r	61dcb74d470162...
/decAES/w1	610af12247dc47...
/decAES/w2	d8a32b94169316...
/decAES/stateMat1	7b678f6383ad8ff...
/decAES/stateMat2	7baf6ff083679c2...
/decAES/stateMat3	031b0617410a1c...
/decAES/rndKey	1211021a32776d...
Now	1900 ps

Features

- Sub modules are all **combinational**.
- Encryption, decryption modules are **sequential**.
- Inputs could be processed only if there are **even** number of hexadecimal characters.
- It takes 12 clock cycles for ecryption and 11 clock cycles for decryption to output the result. Assuming inputs are exactly 128 bit long.
- Zero padding module may take at max 15 additional clock cycles.