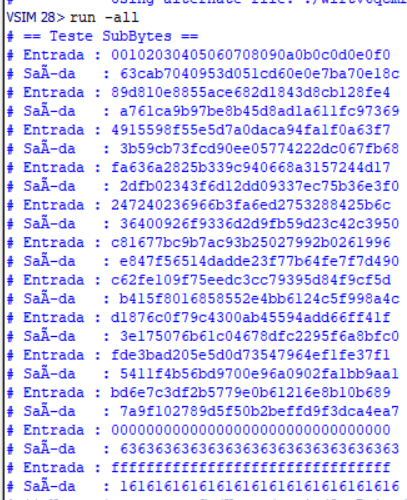
**SUBBYTE - TB**

Módulo SubBytes recebe *start*, processa e entrega *s\_box*. É isso que será verificado no teste (dados do FIPS 197).



round[ 1].start 00102030405060708090a0b0c0d0e0f0

round[ 1].s\_box 63cab7040953d051cd60e0e7ba70e18c

round[ 2].start 89d810e8855ace682d1843d8cb128fe4

round[ 2].s\_box a761ca9b97be8b45d8ad1a611fc97369

round[ 3].start 4915598f55e5d7a0daca94fa1f0a63f7

round[ 3].s\_box 3b59cb73fcd90ee05774222dc067fb68

round[ 4].start fa636a2825b339c940668a3157244d17

round[ 4].s\_box 2dfb02343f6d12dd09337ec75b36e3f0

round[ 5].start 247240236966b3fa6ed2753288425b6c

round[ 5].s\_box 36400926f9336d2d9fb59d23c42c3950

round[ 6].start c81677bc9b7ac93b25027992b0261996

round[ 6].s\_box e847f56514dadde23f77b64fe7f7d490

round[ 7].start c62fe109f75eedc3cc79395d84f9cf5d

round[ 7].s\_box b415f8016858552e4bb6124c5f998a4c

round[ 8].start d1876c0f79c4300ab45594add66ff41f

round[ 8].s\_box 3e175076b61c04678dfc2295f6a8bfc0

round[ 9].start fde3bad205e5d0d73547964ef1fe37f1

round[ 9].s\_box 5411f4b56bd9700e96a0902fa1bb9aa1

round[10].start bd6e7c3df2b5779e0b61216e8b10b689

round[10].s\_box 7a9f102789d5f50b2beffd9f3dca4ea7

teste 0 128’h0

teste 1 128’h1

