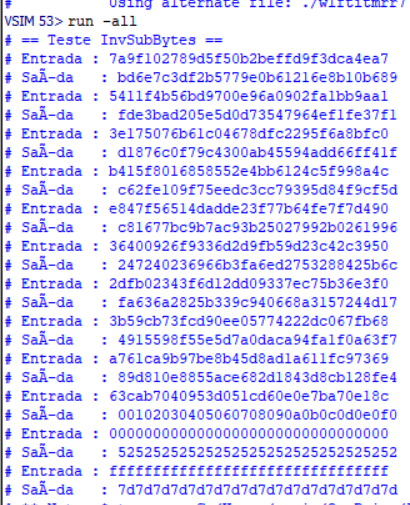
**INVERSE SUBBYTE - TB**

Módulo SubBytes recebe *is\_row*, processa e entrega *is\_box(*state depois InvSubBytes). É isso que será verificado no teste (dados do FIPS 197).

round[ 1].is\_row 7a9f102789d5f50b2beffd9f3dca4ea7

round[ 1].is\_box bd6e7c3df2b5779e0b61216e8b10b689

round[ 2].is\_row 5411f4b56bd9700e96a0902fa1bb9aa1

round[ 2].is\_box fde3bad205e5d0d73547964ef1fe37f1

round[ 3].is\_row 3e175076b61c04678dfc2295f6a8bfc0

round[ 3].is\_box d1876c0f79c4300ab45594add66ff41f

round[ 4].is\_row b415f8016858552e4bb6124c5f998a4c

round[ 4].is\_box c62fe109f75eedc3cc79395d84f9cf5d

round[ 5].is\_row e847f56514dadde23f77b64fe7f7d490

round[ 5].is\_box c81677bc9b7ac93b25027992b0261996

round[ 6].is\_row 36400926f9336d2d9fb59d23c42c3950

round[ 6].is\_box 247240236966b3fa6ed2753288425b6c

round[ 7].is\_row 2dfb02343f6d12dd09337ec75b36e3f0

round[ 7].is\_box fa636a2825b339c940668a3157244d17

round[ 8].is\_row 3b59cb73fcd90ee05774222dc067fb68

round[ 8].is\_box 4915598f55e5d7a0daca94fa1f0a63f7

round[ 9].is\_row a761ca9b97be8b45d8ad1a611fc97369

round[ 9].is\_box 89d810e8855ace682d1843d8cb128fe4

round[10].is\_row 63cab7040953d051cd60e0e7ba70e18c

round[10].is\_box 00102030405060708090a0b0c0d0e0f0

teste 0 128’h0

teste 1 128’h1

