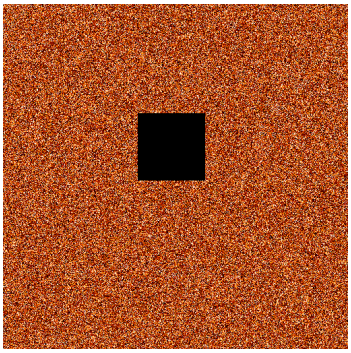
QOE - Quality of Encryption
DM/RAL 11/21

We are concerned about being able to discern any regularities in the output of our Actors ENCRYPTOR blocks.

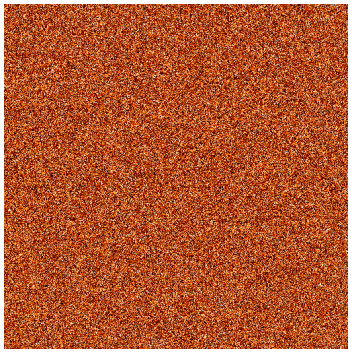
Let's begin with a random field as input data, with a crisp hole punched into it, as a faux message. The noise was derived via iterated SHA3/256 hashing:



And here is the result after encrypting through:

(PIPE (MARSHAL-ENCODER) (ENCRYPTOR EKEY))

where EKEY was randomly generated via SHA3/256 hash:

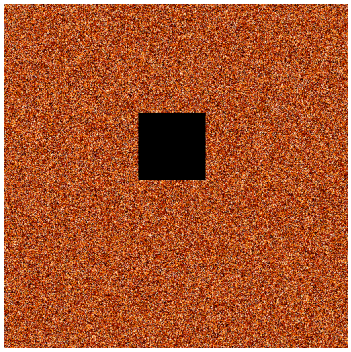


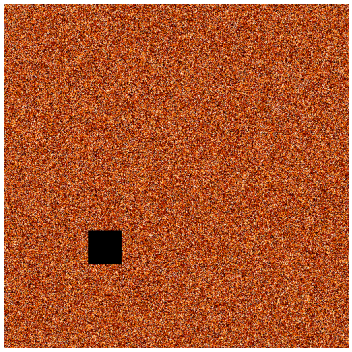
As you can see there are no apparent regularities in the encrypted output. The hole leaves no artifacts in the encrypted output. There is nothing to distinguish it from a random field. The input and output random fields look similar, but not identical.

As a side note, the input data, generated via iterated SHA3/256 hashing, also looks very good as a totally random field. It is a statistically uniform distribution. The encrypted result is similarly from a uniform distribution.

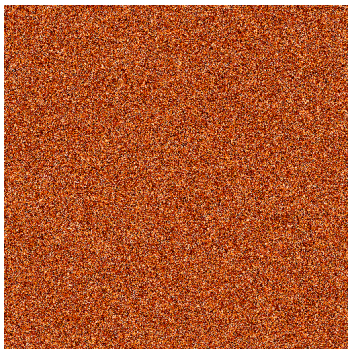
Now, what about the possibility of XOR of two encryptions to recover the XOR of the two original messages, as might be tried by attackers?

Here are two original documents:





And here is the result of XOR between their respective encryption images:



Again, there is no hint of any trace of the original documents.

Using SHA3/256 as the basis for our encryptions allows us to be about as close as one could hope for emulating true one-time pad encryption.