# Double Encryption Q

4 messages

---

**COMINT <comint@gmail.com>** **Fri, Apr 11, 2008 at 4:30 PM**
To: cryptography@metzdowd.com

Quick system scenario:

You have packet [A].

It gets encrypted using an AES algo in a particular mode and we are left with [zA].

More data [B] is added to that encrypted packet.

Now I have [zA]+[B] in one packet and I re-encrypt it with the same algo/key/mode.

Have I just compromised the security somehow? I wasn't aware of anything but something about this double encryption made something ring in my mind so I wanted to double check...

Many thanks,

Mr Pink

---



---

**Jack Lloyd <lloyd@randombit.net>** **Wed, Apr 16, 2008 at 5:16 PM**
Reply-To: cryptography@metzdowd.com
To: cryptography@metzdowd.com

[Quoted text hidden]

This would certainly cause problems in if "particular mode" == OFB or counter, since (if you also reuse the IVs), you could have E(zA) == A.

If you use a different (independent, unrelated) key/IV, then the existence of a weakness in this scheme would seem to provide evidence of an attack on AES, regardless of mode choice.

-Jack

[Quoted text hidden]

---

**Pehr Söderman <Pehrs@kth.se>** **Thu, Apr 17, 2008 at 10:44 PM**
To: COMINT <comint@gmail.com>, cryptography@metzdowd.com

There are some situations when this can be dangerous. It's a matter of implementation. I can directly come up with one trivial scenario that will end you up in trouble:

Assume that you are using AES-CTR (AES in Counter mode) and do not change the IV between the two encryptions. In this case you will correctly encrypt the data, but the second encryption will leave A

unprotected.

/Pehr Söderman

[Quoted text hidden]

---

**Martin James Cochran <Martin.Cochran@colorado.edu>** **Sat, Apr 19, 2008 at 1:09 AM**

To: COMINT <comint@gmail.com>
Cc: cryptography@metzdowd.com

If your original mode of operation is secure, then this should be secure.

The reduction:

Consider algorithm A that tries to break the double encryption mode of operation (DM) in the IND-CPA setting. We can construct an algorithm B that tries to break the original mode of operation (OM) in the IND-CPA setting. B simply runs A and responds to A's queries by querying B's oracle twice to simulate A's oracle, and returning the result. B returns the output of A.

If A breaks the encryption, so does B. So if the original mode is IND-CPA secure, this double encryption should be okay.

Note that the examples given, OCB and CTR with repeated counters, are not IND-CPA secure.

Martin Cochran

[Quoted text hidden]

---