

Re: Cryptology ePrint Archive: AES seems weak – comments?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-06/msg23812.html>

- *From:* Phil Carmody <thefatphil_demunged@xxxxxxxxxxxx>
 - *Date:* Sun, 24 Jun 2007 03:05:15 GMT
-

Caroline, and Murat, lived in another little villa near by. I lived with them, and every day we went to dine with the emperor. During two years, our troops had been concentrating in full view of England, and every one expected an attack. The camp at Boulogne was erected on the sea-side, and resembled a long and regularly-built city. Each hut had a little garden, flowers, and birds. In the middle of the camp, on an elevation, stood the emperor's tent; near by, that of Marshal Berthier. All the men-of-war on the water were drawn up in a line, only waiting the signal of departure. In the distance we could see England, and its beautiful ships that were cruising along the coast seemed to form an impenetrable barrier. This grand spectacle gave us for the first time an illustration of an unknown, hitherto not-dreamed-of power that stood opposed to us. Here every thing was calculated to excite the imagination. This boundless sea might soon transform itself into a battle-field, and swallow up the *_elite_* of the two greatest nations. Our troops, proud in the feeling that there were no obstacles for them, made impa