

Attack Mode examples with simple cipher?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-08/2017.html>

From: flip (*flip_alpha_at_safebunch.com*)

Date: 08/31/04

Date: Mon, 30 Aug 2004 18:27:57 -0700

Hello,

I was wondering if anyone has done simple examples using something like a shift cipher (or even a reduced round symmetric cipher) to show example of a ciphertext, chosen ciphertext, plaintext, ... attack?

I was thinking that a simple example of each of these could go a long way in helping people get the points.

Does anyone know if something like this has been done (on searching google, I found all kinds of attacks related to papers for linear differential and all variants), but just wanted some easy example like those mentioned above.

Any thoughts or pointers appreciated.

Thanks.