

Weak keys in Blowfish revisited

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-05/5479.html>

From: David (david_sorg_at_hotmail.com)

Date: 05/31/04

Date: 30 May 2004 21:15:30 -0700

If I do pick one of these weak keys at random (the 1 in 2^{88} keys), can somebody detect that a weak key was used? If the attacker didn't have the ability to launch a chosen plaintext or chosen ciphertext attack, would the encryption still be secure?