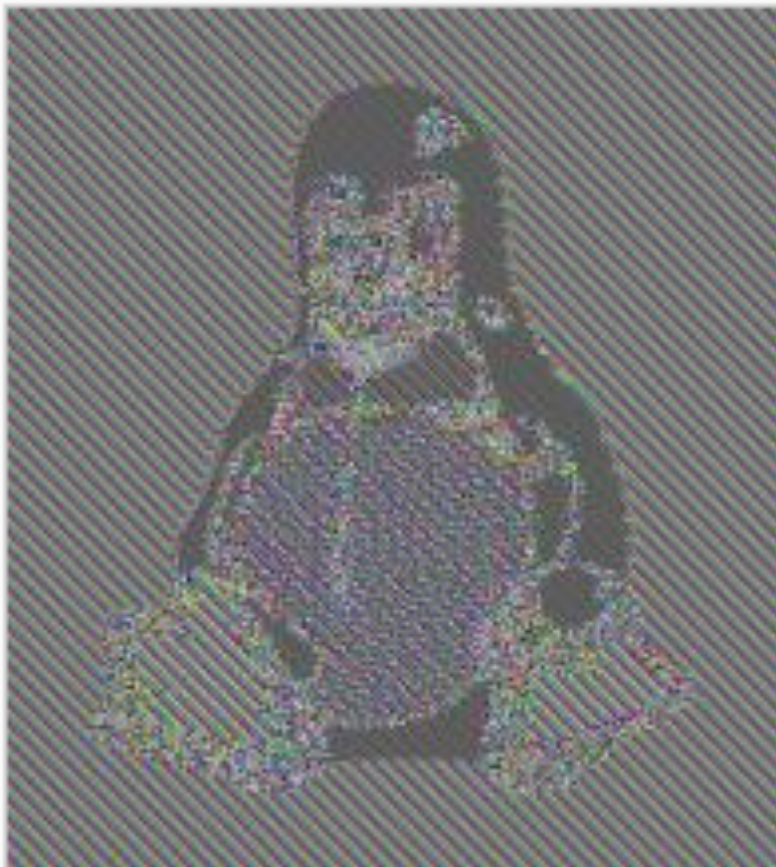


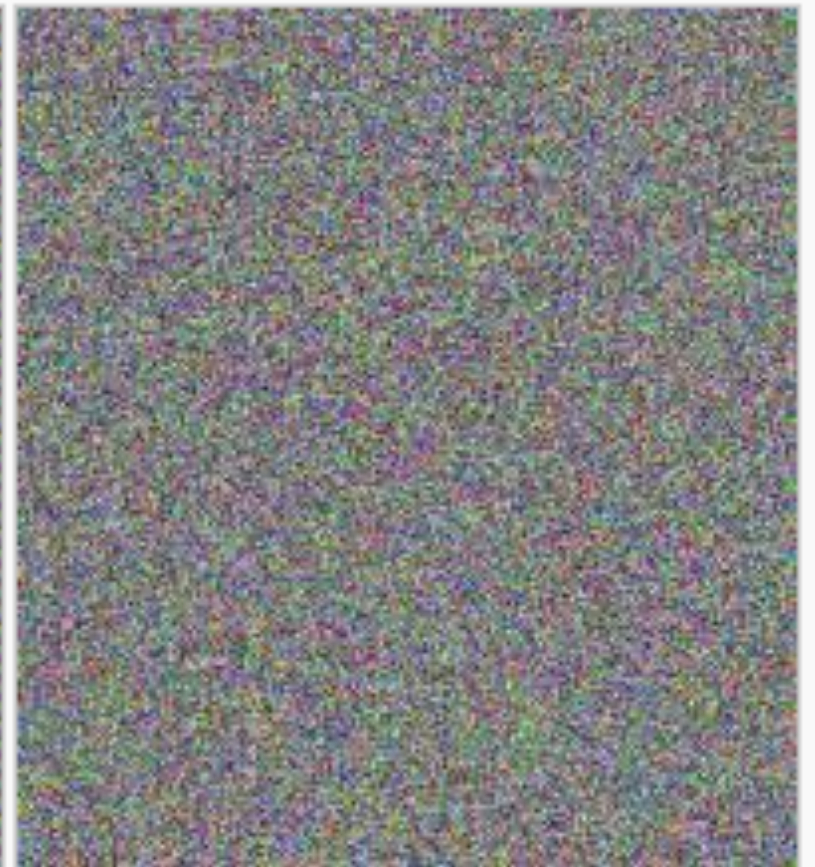
How bad is ECB mode with a large data?



Original image



Encrypted using ECB mode



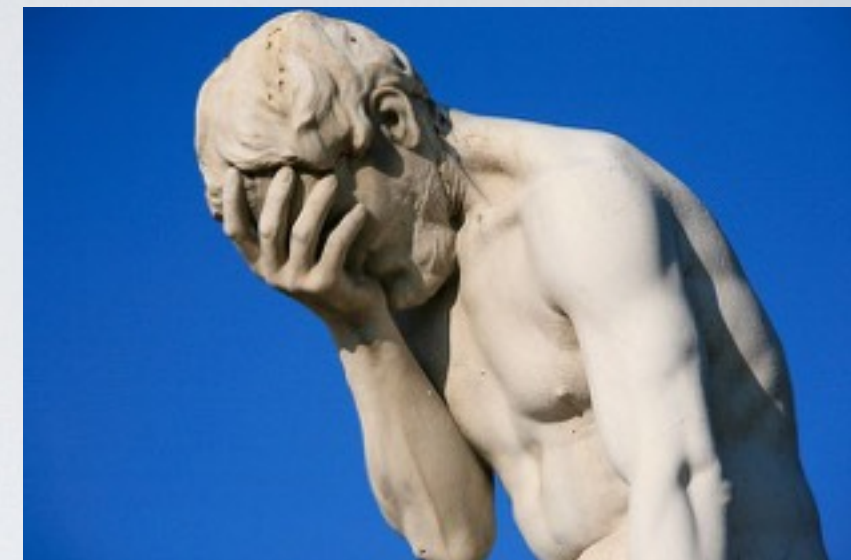
Modes other than ECB result in pseudo-randomness

source: *Wikimedia*

HACKERS RECENTLY LEAKED **153 MILLION** ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS. ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:

| USER | PASSWORD | HINT | |
|-------------------|------------------|---|----------------------|
| 4e18acc1ab27a2d6 | | WEATHER VANE SWORD | <input type="text"/> |
| 4e18acc1ab27a2d6 | | | <input type="text"/> |
| 4e18acc1ab27a2d6 | a0a2876eb1ea1fca | NAME 1 | <input type="text"/> |
| 8babbb6299e06eb6d | | DUH | |
| 8babbb6299e06eb6d | a0a2876eb1ea1fca | | <input type="text"/> |
| 8babbb6299e06eb6d | 85e9da81a8a78adc | 57 | |
| 4e18acc1ab27a2d6 | | FAVORITE OF 12 APOSTLES | |
| 1ab29ae86da6e5ca | 7a2d6a0a2876eb1e | WITH YOUR OWN HAND YOU HAVE DONE ALL THIS | |
| a1f9b2b6299e7a2b | e0dec1e6ab797397 | SEXY EARLOBES | <input type="text"/> |
| a1f9b2b6299e7a2b | 617ab0277727ad85 | BEST TOS EPISODE | <input type="text"/> |
| 39738b7adb0b8af7 | 617ab0277727ad85 | SUGARLAND | |
| 1ab29ae86da6e5ca | | NAME + JERSEY # | |
| 877ab7889d3862b1 | | ALPHA | <input type="text"/> |
| 877ab7889d3862b1 | | | <input type="text"/> |
| 877ab7889d3862b1 | | | <input type="text"/> |
| 877ab7889d3862b1 | | OBVIOUS | <input type="text"/> |
| 877ab7889d3862b1 | | MICHAEL JACKSON | <input type="text"/> |
| 38a7c9279codeb44 | 9dca1d79d4dec6d5 | | |
| 38a7c9279codeb44 | 9dca1d79d4dec6d5 | HE DID THE MASH, HE DID THE | <input type="text"/> |
| 38a7c9279codeb44 | | PURLOINED | <input type="text"/> |
| 08ae5745a7b7af7a | 9dca1d79d4dec6d5 | FAV. LATER-3 POKEMON | |

THE GREATEST CROSSWORD PUZZLE
IN THE HISTORY OF THE WORLD



source: XKCD