1&0 cipher

Invented by Giacomo Tommaso Petrucci

After 10 years of hard research in the filed of cryptography, I found the answer to the modern need of privacy and security. The idea behind this cipher is at the same time easy and groundbreaking: process the input in binary mode substituting 1s with 0s and 0s with 1s. This new approach has several advantages:

- ⭐ 100% KISS rule compliant
- ⭐ Easily computable by hand: you will never again be stopped by your laptop's battery running out of charge or your linux box complaining about a kernel panic. All you need to crypt/decrypt is an ASCII table and a bunch of minutes. Compared to other modern ciphers, this approach is 100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 times faster (trust me, I've actually calculated it. I swear I didn't kept the “0” button pressed for a random amount of time)
- ⭐ Easy to understand. If you try to understand modern ciphers like rijndael you will end having a strong headache in five minutes. This cipher instead can be fully understood even by an elementary school child. This cipher is easy to implement as well
- ⭐ Free to use. Since you will not having headaches, you wouldn't have to spend money on drugs, so it's completely free of charge
- ⭐ Keyless. Most other ciphers are intrinsically weak because they rely on a key: leak it and your data can be read by anyone. Some ciphers (eg GPG) asks you to crypt your key using another key but this is just a way to hide the problem and make things harder (KISS rule non compliant). Without a key there's no way you can leak it: even if someone tries to force you to reveal it all you can say is “I'm sorry, there's no key”[1]. This feature also makes it brute force resistant since there's no key to brute force
- ⭐ Resistant to all sorts of cryptanalysis[2]. Most cryptanalysts won't even think that to decrypt it you have to substitute 1s with 0s and 0s with 1s and even the few that

1 Some scholars argue that using this cipher you are just doing bitwise operations using “1” as key. Don't trust them, they just envy me.

2 It may be vulnerable to deletion cryptanalysis (http://www.anagram.com/jcrap/Volume_0_0/crv0n0-1.pdf), but since this attack is explicitly forbidden by 1&0 cipher's terms of use you don't have to worry about it.

would consider that would look somewhere else after a few seconds because "It's too easy, it couldn't be that"

- ⭐ It's an Italian cipher and you know, everybody likes Italian products

But why I'm so sure it's so secure? Well, before submitting it to Snake Oil Competition I've sent my findings to NSA (I know that they are the enemy, but you know, they gave me big bucks...). They found my paper so valuable and strategically critic that as soon as they finished to read it, they decided to encrypt it using 1&0 cipher. But shortly after they forgot how to decrypt it, so they both have and don't have my paper. They asked Heisenberg and Schrödinger for a solution but still haven't found one.

I've written an Assembly implementation of this fantastic and unbreakable cipher for the Pentium II MMX, the reference platform chosen by Snake Oil Crypto Competition:

eqvceyiwcwegcfiewcbhwcvuegoewhfiurefe

44363yrefbciewfowefwecbòVIUÈEAÀA

bgurebfgoirebgrttor hoittroir hrthrtugh8t9ghfo

fuyerfgeiufgrefgehfvdc87ewf34r43vf54g54hogp9g54

ewuifvgifveivuebewuffh43yt43oth984thskvbbiòreòa

rwyugoyutgerfnvrouehrejbvhbuoronbsbjnrioberàbtio

cewufewyufew

giufhgtjgtrb

frifrhfreforbefgreiufhrhfvhuire

Since I'm a cryptologist, the above code is encrypted with one-time pad. "So how I find the key to read it?" you may wonder. It's easy: just write an ASM implementation of 1&0 cipher for the Pentium II MMX and compute the key as the difference between yours and above code. Following exactly the same approach, you can find the C implementation I've just written. That's cool, isn't it? Another cool feature is that the Assembly version runs at a speed of about $3x10^8$ m/s [3].

WARNING: a Chinese heard about my cipher and tried to copy it. His approach is the opposite as mine: he substitutes 0s with 1s and 1s with 0s (I instead substitute 1s with 0s

3 If you're a physicist and you are complaining because this is the speed of light and m/s isn't a suitable unity measure for computer program's speed, then stop it. When it will came to physics I will ask for your opinion but as long as we talk about cryptography I'm the expert here, not you.

and 0s with 1s). Since I've proved that my approach is safe and he is doing the opposite, follows that his cipher (called 0&1 cipher) is unsafe and easily breakable. I know that for a given input the output looks the same, but *it is not* the same. Result isn't the only thing that counts, it is equally important how you get it. Consider yourself warned.

CONCLUSIONS

This cipher proved to be so secure that one day could replace rijndael as Advanced Encryption Standard or, in short, AES. In the mean time keep away from non original copies, expecially Chinese ones since they are not secure. This paper was started on 15/8/2015 and finished on 16/8/2015 and sent to Snake Oil Crypto Competition on the same day. I hope the ~~high bribe~~ kind donation I sent them helps the commission in the evaluating process.