ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023
CRYPTOGRAPHY, 2022, assignments list # 2, 14.3.2023

1. Assume that you have a hash function $H : \{0,1\}^{512} \longrightarrow \{0,1\}^{160}$. However, for your application, you need a function $H' : \{0,\ldots,p-1\} \longrightarrow \{0,\ldots,q-1\}$ for some prime numbers p and q. How to customize H to get H' that has similar properties?

2. Consider the Meyer-Davies scheme. The encryption function E encrypts 80-bit blocks.

   - evaluate the complexity of finding a collision for this scheme applied directly for E (an estimation is enough),
   - adjust it (how?) to create secure hashes of length 160.

3. You need to create a key for your cryptocurrency wallet – a random 256 bit number that will be used for signing. You have a hardware cryptocurrency wallet D. The device D can import a key, but is protected against exporting the key.

   You are afraid that your cryptocurrency assets will be lost once D crashes (every device eventually crashes in an unexpected moment). So you keep a paper copy of the key.

   There are challenges: if you have a long sequence of bits, then it is very likely that what you input is not the same as what you have on the paper copy.

   - Design a scheme for codes on paper that enable easy and reliable recovery from a security copy on paper to the secret signing key (mnemonic codes).
     Be aware of cultural threats (for example, a Chinese will never enter a digit 4 into the code, Polish guys are likely to use curse words, . . .)
   - check how the problem has been solved by the BIP-39 standard used in cryptocurrency communities.

4. Consider the function $F(x, y, z) = (x \wedge y) \vee (\bar{x} \wedge z)$ used by MD5. What would be the effect of replacing it with $F(x, y, z) = (x \wedge y) \vee (x \wedge z)$ in the context of finding MD5 collisions?

5. Consider a modification of MD5 where each 32-bit block of message is used only once (it is equal to exactly one w_j). What would be the consequences for finding a collision?

/-/ Mirosław Kutyłowski