

Počítačová algebra - 2. DÚ

1. listopadu 2023

Příklad 1. Rozluštěte následující zprávu (ASCII znaky, zapsané v hexadecimální soustavě) zašifrovanou RSA-1024:

$c = 0x4f7a74ab7da5b0a448c99317e3afb2ba2b50e78639c39039000a5bd900c8d6c0bd2834b140c643a7c6d1928bfbf06c5e8bfea7a3c7ddf5a9f5a8cb387b0d56b9d03e5893e9d292aece7538c493d7a5f17eb3e6e7ecc2bd68bcf045d9c71b92d0685d050f847b436a3bd994da9e0375d70789fcc101e8494f31818ee39ee5690a$

s následujícími veřejnými parametry

$N = 0x8610a01d832e697a9f5dd31fd36cfd96e10c2594876e6f831a74ba11a1392f8ab205c9eba464c4515d1bb4a15820a37057030fa385cddacbf8d0eb60c083cdc488f7cb360dd00281877f0f35983a51cd489b10fd53387fff0eeeeef0b6fda12ecde457bf899d559925bb0bee07d0110435e162d4c54328f0ac029eada56403f3,$
 $e = 0x10001.$

Následující veřejné klíče byly vygenerovány pomocí stejného generátoru náhodných čísel. $N_1 = 0x7720f8e16ce58bfd2da783b1df7f470c356d7250c75a402aa98ed5c76977d7bb40f7aeb68b98bafcd2d29088a477dcd6d0f0e4f9433ca4ab8d62941769d005f76a67c3fce01f07f2e228abd5457762d4610d907d4369add2ade45a7b8edf4dafae331c4df016e318fdd66931daf8e492a75e60cbc0460c553bfee08de9c98465$

$N_2 = 0xb03b3ea93fb954b045dcb3212aab589103020045ef21917b6fe323a5b1f2fa6818c816935c068f1c7269fe11cfb8687e64c8be78400e2ebb013ac5fc757f4a5190b0789d0eb7abbd01a90108f82c369406d5817877865dfb7099511b4e215a0d106b88bf127c2992f772e360b011fbda71febffe02374674a9b5d4a60231abd7$

Tento článek by vám mohl pomoci: <https://www.iacr.org/archive/crypto2012/74170620/74170620.pdf>
Rozluštěnou zprávu zašlete na email: [jiri.pavlu294\(zavináč\)gmail.com](mailto:jiri.pavlu294(zavináč)gmail.com)