The security of this system is based on the assumption that knowing the encrypting keys n and e does not allow one to compute the decrypting keys n and d. However, there are algorithms for doing exactly that! In fact, if p and q are so large that their binary rep- resentations require hundreds of digits, then the best known factoring algo- rithms would require years before the identities of p and q could be revealed from n. In turn, the content of an encrypted message would remain secure long after its significance had deteriorated.