1) Alice has published two public keys with the same modulus: \((n, e_1)\) and \((n, e_2)\). Bob does not know which one of the two keys he should use, hence he sends two cryptotexts

\[ y_i = x^{e_i} \pmod{n} \quad (i = 1, 2) \]

to Alice. The eavesdropper Eve manages to capture both cryptotexts. How can she find the plaintext \(x\) if we assume that \(\gcd(e_1, e_2) = 1\)? What can we learn from this?

2) The public RSA keys of Huey, Dewey and Louie are \((n_1, 3)\), \((n_2, 3)\) and \((n_3, 3)\). Uncle Donald sends the same message \(x\) to all three nephews, encrypted using their public keys. Eve manages to capture all three cryptotexts

\[ y_i = x^3 \pmod{n_i} \quad (i = 1, 2, 3). \]

How can Eve break Uncle Donald’s encryption and find the plaintext \(x\)?

Hint: the Chinese remainder theorem tells us that a solution \(x\) can efficiently be found to a system of congruences

\[
\begin{align*}
    x &\equiv a_1 \pmod{n_1} \\
    x &\equiv a_2 \pmod{n_2} \\
    \vdots \\
    x &\equiv a_k \pmod{n_k}
\end{align*}
\]

under the assumption that the numbers \(n_i\) and \(n_j\) are pairwise coprime, i.e. \(\gcd(n_i, n_j) = 1\). Furthermore, the solution is unique modulo \(n_1n_2\cdots n_k\).

3) Bob wants to use RSA and he has chosen numbers \(p = 47\) and \(q = 57\). Encrypt message \(x = 3\) (to be sent to Bob) and then show Bob how to decrypt the message when

(a) \(e = 89, d = 521\);
(b) \(e = 11, d = 1171\).

What happened?

4) The public key of Alice is \((n, e) = (150419, 379)\). Eve has managed to find out that Alice’s private key is probably \(d = 13819\). Help Eve to find factors of \(n\).

5) Let us define a function \(h\) as follows. The length of the output \(h(x)\) is fixed to \(n\). Now we first divide the input \(x\) (that is assumed to be a bit string of an arbitrary length) into blocks of size \(n\). The last block is padded with zeros if necessary. Let \(x_0x_1\ldots x_k\) be the padded representation of \(x\) in \(n\)-bit blocks. We define \(h(x) = x_0 + x_1 + \ldots + x_k \pmod{2^n}\). Which of the properties of a hash function are fulfilled by \(h\)?

6) Suppose \(n = pq\) where both \(p\) and \(q\) are (secret and distinct) strong primes; \(p = 2p_1 + 1\), \(q = 2q_1 + 1\). Assume further that \(g\) is an element of order \(2p_1q_1\) in \(\mathbb{Z}_n^*\). (This is actually the largest possible order in \(\mathbb{Z}_n^*\), i.e. \(\mathbb{Z}_n^*\) is not cyclic.)

Define a hash function \(h : \{1, \ldots, n^2\} \to \mathbb{Z}_n^*\) by the rule \(h(x) = g^x \pmod{n}\). Suppose now that \(n = 603241\) and \(g = 11\) are used to define a hash function of this type. Suppose further that three collisions are found for \(h\): \(h(1294755) = h(80115359) = h(31980639)\).

Use this information to find factors of \(n\).