Example 151. (warmup) When using RSA, why must we never directly encrypt messages that can be predicted (like "yes", "no", "maybe"; or a social security number)?

Solution. Because an attacker can make a list of likely messages (for instance, a list of all possible social security numbers) and encrypt all of them using the public key. As soon as one of these matches the ciphertext, the attacker has broken the message.

Comment. This applies to any public key cryptosystem, in which a message gets encrypted in a single way. To avoid this issue, some randomness is typically introduced. For instance, for RSA, when used in practice, the plaintext would be padded with random noise before encryption. On the other hand, the ElGamal encryption we discuss next, has such randomness already built into it.

Comment. Note that this is not an issue with symmetric ciphers like DES or AES. In that case, even if the attacker knows that the plaintext must be one of "0" or "1", she still cannot draw any conclusions from intercepting the ciphertext.

Example 152. (warmup) Bob's public RSA key is $N=33$, $e=3$.

(a) Encrypt the message $m=4$ and send it to Bob.

(b) Determine Bob's secret private key d.

(c) You intercept the message $c=31$ from Alice to Bob. Decrypt it using the secret key.

Solution.

(a) The ciphertext is $c=m^e \pmod N$. Here, $c\equiv 4^3=64\equiv 31 \pmod{33}$. Hence, $c=31$.

(b) $N=3\cdot 11$, so that $\phi(N)=2\cdot 10=20$.
To find d, we need to compute $e^{-1} \pmod{20}$. Since the numbers are so simple we see $3^{-1}\equiv 7 \pmod{20}$. Hence, $d=7$.

(c) We need to compute $m=c^d \pmod N$, that is, $m=31^7\equiv(-2)^7\equiv 4 \pmod{33}$.
That is, $m=4$ (as we already knew from the first part).

Theorem 153. Let $N=pq$ and d,e be as in RSA. Then, for any m, $m\equiv m^{de} \pmod N$.

Comment. Using Euler's theorem, this follows immediately for residues m which are invertible modulo N. However, it then becomes tricky to argue what happens if m is a multiple of p or q.

Proof. By the Chinese remainder theorem, we have $m\equiv m^{de} \pmod N$ if and only if $m\equiv m^{de} \pmod p$ and $m\equiv m^{de} \pmod q$.
We can write $de=1+(p-1)a$ for some integer a. By little Fermat, it follows that $m^{de}=m^{1+(p-1)a}\equiv m \pmod p$ for all m that are invertible modulo p. On the other hand, if m is not invertible modulo p, then this is obviously true (because both sides are congruent to 0). Thus, $m\equiv m^{de} \pmod p$ for all m.
Likewise, modulo q. □

Armin Straub
straub@southalabama.edu

Theorem 154. Determining the secret private key d in RSA is as difficult as factoring N.

Proof. Let us show how to factor $N = pq$ if we know e and d.

- First, let t be as large as possible such that 2^t divides $ed-1$. (Note that $t \geqslant 2$. Why?!)
  Write $m = (ed-1)/2^t$.
- Pick a random invertible residue a. Observe that $a^{ed-1} \equiv 1 \pmod{N}$. In particular, $(a^m)^{2^t} \equiv 1$.
  Hence, the multiplicative order of a^m must divide 2^t.
- Suppose that a^m has different order modulo p than modulo q. (Both orders must divide 2^t.)
  [This works for at least half of the (invertible) residues a. If we are unlucky, we just select another a.]
- Suppose a^m has order 2^s modulo p, and larger order modulo q.
  Then, $a^{2^s m} \equiv 1 \pmod{p}$ but $a^{2^s m} \not\equiv 1 \pmod{q}$. Consequently, $\gcd(a^{2^s m} - 1, N) = p$.
- Of course, we don't know s (because we don't know p and q), but we can just go through all $s = 1, 2, \ldots, t-1$. One of these has to reveal the factor p. □

However. It is not known whether knowing d is actually necessary for Eve to decrypt a given ciphertext c. This remains an important open problem.

Example 155. (homework) Bob's public key is $N = 323$, $e = 101$. Knowing $d = 77$, factor N using the approach of the previous theorem.

Solution. Here, $de - 1 = 7776$, which is divisible by 2^5. Hence, $t = 5$ and $m = 243$.

- Let's pick $a = 2$. $a^m = 2^{243} \equiv 246 \pmod{323}$ must have order dividing 2^5.
  $\gcd(246^2 - 1, 323) = 19$ (so we don't even need to check $\gcd(246^{2^s} - 1, 323)$ for $s = 2, 3, 4$)
  Hence, we have factored $N = 17 \cdot 19$.

Comment. Among the $\phi(323) = 16 \cdot 18 = 288$ many invertible residues a, only 36 many would not lead to a factorization. The remaining 252 residues all reveal the factor 19.

Another project idea. Run some numerical experiments to get a feeling for the number of residues that result in a factorization.