Example 136. 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).

Example 137. (extra) Bob's public RSA key is $N=55$, $e=7$.

(a) Encrypt the message $m=8$ and send it to Bob.

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

(c) You intercept the message $c=2$ from Alice to Bob. Decrypt it using the secret key.

Solution.

(a) The ciphertext is $c=m^e \pmod N$. Here, $c\equiv 8^7 \pmod{55}$
$8^2\equiv 9$, $8^4\equiv 9^2\equiv 26$. Hence, $8^7=8^4\cdot 8^2\cdot 8\equiv 26\cdot 9\cdot 8\equiv 2 \pmod{55}$. Hence, $c=2$.

(b) $N=5\cdot 11$, so that $\phi(N)=4\cdot 10=40$.
To find d, we compute $e^{-1} \pmod{40}$ using the extended Euclidean algorithm:

$$\begin{aligned} & \gcd(7,40) && \boxed{40} &= 6\cdot\boxed{7}-2 \\ = \ & \gcd(2,7) && \boxed{7} &= 3\cdot\boxed{2}+1 \\ = \ & 1 \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$1=\boxed{7}-3\cdot\boxed{2}=\boxed{7}-3\cdot\left(6\cdot\boxed{7}-\boxed{40}\right)=-17\cdot\boxed{7}+3\cdot\boxed{40}.$$

Hence, $7^{-1}\equiv -17\equiv 23 \pmod{40}$ and, so, $d=23$.

(c) We need to compute $m=c^d \pmod N$, that is, $m=2^{23} \pmod{55}$.
$2^2=4$, $2^4=16$, $2^8\equiv 36\equiv -19$, $2^{16}\equiv 19^2\equiv 31 \pmod{55}$. Hence, $2^{23}=2^{16}\cdot 2^4\cdot 2^2\cdot 2\equiv 31\cdot 16\cdot 4\cdot 2\equiv 8 \pmod{55}$.
That is, $m=8$ (as we already knew from the first part).

Example 138. RSA is so cool! Why do we even care about, say, AES anymore?

Solution. RSA is certainly cool, but it is very slow (comparatively). As such, RSA is not practical for encrypting larger amounts of data. RSA is, however, perfect for sharing secret keys, which can then be used for encrypting data using, say, AES.

Example 139. Is it a problem that $m=1$ is always encrypted to $c=1$? (Likewise for $m=0$.)

Solution. Well, it would be a problem if we reply to questions using YES (say, 1) and NO (say, 0) and encrypt our reply. However, this would always be a terrible idea in any deterministic public key cryptosystem (that is, a system, in which a message gets encrypted in a single way)!

Why? That's because Eve can just encrypt both YES and NO (or any collection of expected messages) and see which matches the ciphertext she intercepted.

Important conclusion. We must not send messages taken from a small predictable set and encrypt them using a deterministic public key cryptosystem like RSA.

Once realized, this is easy to fix: for instance, Alice can just augment the plaintext with some random garbage in such a way that Bob can discard that garbage after decryption. This is done when RSA is used in practice.

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 140. For his public RSA key, Bob needs to select p, q and e. Which of these must be chosen randomly?

Solution. The primes p and q must be chosen randomly. Anything that makes these prime more predictable, makes it easier for an attacker to get her hands on them [in which case, the secret key d is trivial to compute].

On the other hand, e does not need to chosen at random. In fact, the next result shows that knowing any pair e, d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$ would allow us to factor $N=pq$ (and thus break).