Fkdswhu 5.4
Wkxuvghb, Zhhn 4

Warmup

Compute:

1. $18 + 9 \pmod{26}$
2. $22 + 21 \pmod{26}$
3. $24 \cdot 5 - 7 \pmod{26}$

For which of these functions $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ does an inverse function exist? Give the inverse if it exists.

1. $f(x) = x$
2. $f(x) = x + 3$
3. $f(x) = 3x$
4. $f(x) = 4x$
5. $f(x) = 13x + 7$
6. $f(x) = 7x + 13$

RSA

The actors involved in the process:

1. Alice, who has the public key and the only one who knows the private key.
2. Bob wants to send a message to Alice.
3. Eve is the eavesdropper, who wants to get hold of Bob's message.

The relevant numbers used in the encryption/decryption process:

1. (n, e): Alice's RSA public key.
2. m, the number ("message") that Bob wants to encrypt and send to Alice.
3. $n = pq$: the factorization of n, which only Alice knows. p and q are large prime numbers (say, 300 digits).
4. $\varphi(n) = (p-1)(q-1)$, the number of elements relatively prime to n. In other words, the number of elements in the group $\mathbb{Z}_n^\times$.
5. e is the exponent of encryption, a number such that $\gcd(e, (p-1)(q-1)) = 1$. (So, $e \in \mathbb{Z}_n^\times$.)
6. d is the exponent of decryption, a number such that $de \equiv 1 \pmod{(p-1)(q-1)}$.

The process:

1. Bob takes his number m and computes $m^e \pmod{n}$. He then sends this new number to Alice.
2. Alice then raises this number to the exponent d, getting $m^{ed} \pmod{n}$.
3. Since $de \equiv 1 \pmod{(p-1)(q-1)}$, $de = 1 + k(p-1)(q-1)$ for some integer k. This leads to the congruences

$$m^{de} \equiv m^{1+k(p-1)(q-1)} \equiv (m^{(p-1)})^{k(q-1)} \cdot m \equiv m \pmod{p}$$
$$m^{de} \equiv m^{1+k(p-1)(q-1)} \equiv (m^{(q-1)})^{k(p-1)} \cdot m \equiv m \pmod{q},$$

   at which point the Chinese Remainder Theorem implies $m \equiv 1 \pmod{pq}$, and so $m \equiv 1 \pmod{n}$. Alternatively, we could show this directly by saying

$$(m^{(p-1)(q-1)})^k \cdot m \equiv (m^{\varphi(n)})^k \cdot m \equiv m \pmod{n}.$$

   Either way, Alice now has Bob's message successfully decrypted.

One key to security: Even if Eve gets access to $c = m^e$ and manages by other means to learn m, then she would still have to solve $c^x \equiv m \pmod{n}$, which is hard.

Chosen Ciphertext Attack

Eve has $c = m^e$, and she wants m. Pick some random number r such that $r < n$. Then compute

$$\begin{aligned} x &= r^e \mod n \\ y &= xc \mod n \\ t &= r^{-1} \mod n \end{aligned}$$

Then sends y to Alice and asks her to put her digital signature on it. Alice agrees, returning $u = y^d \pmod{n}$. Then Even computes

$$tu \mod n = r^{-1}y^d \mod n = r^{-1}x^d c^d \mod n = r^{-1}(r^e)^d m \mod n = m$$

Eve now has m. Lesson: do not use your private key to sign mysterious messages.