Sending a Secret Message in Modern Era using ideas from 1736

Chockalingam wished to send Nafisa a message M that he wished Nafisa and no one else to read. They lived in a public key system. Chockalingam got Nafisa's public key and encrypted the message M using Nafisa's public key to obtain an encrypted message c. He sends this to Nafisa. Upon receiving the message from Chockalingam, Nafisa decrypts it using her private key. No one else can decrypt the message unless they have Nafisa's private key.

Can this be done in Practice ?

1. *Congruences:* Let $n \in \mathbb{N}$ and $x, y \in \mathbb{Z}$. We say $x \sim_n y$ if $x - y$ is divisible by n. Usually denoted by $x \equiv y \mod n$.
   (a) Show that $\sim_n$ is an equivalence relation on $\mathbb{Z}$.
   (b) The equivalence relation partitions $\mathbb{Z}$ into n congruence classes given by $\bar{r} := \{nk + r | k \in \mathbb{Z}\}$ for $0 \leq r \leq n$.
   (c) Let $\mathbb{Z}_n = \{\bar{r} : 0 \leq r \leq n-1\}$. Define addition modulo n by
   $$\bar{a} +_n \bar{b} = \overline{a+b}.$$
   Show that $\mathbb{Z}_n$ equipped with $+_n$ is an abelian group.
   (d) Let $\mathbb{Z}_n^\times = \{\bar{r} : 1 \leq r \leq n-1, \text{ such that } r \text{ is relatively prime to } n\}$. Define product modulo n by
   $$\bar{a} \cdot_n \bar{b} = \overline{a \cdot b}.$$
   Show that $\mathbb{Z}_n^\times$ equipped with $\cdot_n$ is an abelian group.
2. *Totient Function:* For $n \in \mathbb{N}$, let $\phi(n) = \mid \mathbb{Z}_n^\times \mid$
   (a) If n is a prime then find $\phi(n)$.
   (b) If $n = pq$ where p and q are prime then find $\phi(n)$.
   (c) Can you write down a prescription on how to find $\phi(n)$?
3. *Euler's Theorem (1736):* Let $1 \leq a < n$ be such that a, n are relatively prime. Show that
   $$a^{\phi(n)} \equiv 1 \mod n.$$
4. *RSA:* Let $n = pq$ where p, q are primes with $p < q$. Assume Chockalingam's message is M with $2 \leq M \leq p-1$. Need to find a public key (e, n) that Nafisa can share so that Chockalingam can encrypt M with F and send
   $$c = M^e \mod n$$
   in the public channel. We also need to provide her with private key be (d, n) so that she can decrypt c using G and find
   $$M = c^d \mod n.$$
   (a) Can you suggest a procedure to find e and d that enables encryption and decryption ?
   (b) Snoopkutty and Doddasnoop are tracking the public channel communication. They know c, e, n and they are trying to find d to get to M. Is there a way to make it impossible in their lifetime if they do it by hand ?
   (c) Do the computation for the following example: $p = 17, q = 5$ and $M = 6$.