Comments on Chapter 7

Who does what using whose keys?

Suppose there are a number of users in the communication network (such as the internet). Let them be user $1, 2, 3, \cdots$, etc.

Each user i has to pick his/her own public and private keys. So, each will pick p_i, q_i, and calculate $N_i = p_i q_i$ and e_i coprime to $(p_i - 1)(q_i - 1)$, and d_i satisfying $e_i d_i \equiv 1 \mod (p_i - 1)(q_i - 1)$. For example, if there are 100 users, there will be 100 pairs of public and private keys.

Suppose user i wants to send a message M to user j.

- To encrypt, user i encrypts by using user j's public key (e_j, N_j).
- To decrypt, user j decrypts by using his/her own private key (d_j, N_j).
- To sign, user i uses his own private key (d_i, N_i).

We can understand, rather than remember all these.

A message is encrypted for a specific receiver, but every sender has follows the same encryption procedure. So, it must use the receiver's key. Furthermore, everyone can do it, so, it must use the public key.

Likewise, only the receiver can decrypt. So, decryption must use the private key of the receiver.

Now, a signature has nothing to do with the receiver, and verifies who is the sender. So, it has to use the sender's key, and since only the sender can sign, it has to use the private key.

What's in the last half page of Chapter 7 (p 179) concerning digital signature?

It assumes knowledge of Chapter 6. We summary the concepts here.

> A function f acting on a set of numbers is a prescribed way to transform these numbers.
> For example, $f(x) = 2x$ takes x to $2x$.
> We say that g inverts f if g "undoes" the action of f.
> Example 1: if $f(x) = 2x$ in the set $\mathbb{R}$, then $g(y) = \frac{1}{2}y$ inverts f (since $g(f(x)) = \frac{1}{2}f(x) = \frac{1}{2}2x = x$).
> Example 2: if $f(x) = 2x$ in the set $\mathbb{Z}_5$, then $g(y) = 3y$. (Check this!).
> More abstractly, we call a function g the inverse of f if $g(f(x)) = x$ for all x in the set we consider.
> Note that some functions have no inverse. For example, $f(x) = 2x$ has no inverse in the set $\mathbb{Z}$ or $\mathbb{Z}_6$. Chapter 6 (esp 6.1-6.5) is not covered in Ma135, but you will find it useful reading exercise.

For each receiver j, the encryption process is a function acting on the set of all possible plaintexts (ranging from 0 to $N_j - 1$). It takes the plaintext M to the ciphertext $C = f(M) = M^{e_j} \mod N_j$. The decryption map should take $C = f(M)$ back to M, therefore, it is the inverse of the encryption map. Using the above terminology, the inverse of f is $g(C) = C^{d_j} \mod N_j$. Note that I've left all the sub-j's around, to remind you that encryption is part of a communication procedure, always involving a sender and a receiver involved (this is only implicit in the text).

In the second half of p 179: Ursula is the sender and (e, N), (d, N) are her public and private keys. When the book says u is her encryption function, it means other people apply that encryption function to encrypt messages intended for her. (She never encrypts things for herself!) Here $u(M) = M^e \mod N$. The inverse function is labeled as u^{-1} (what we call g in the box). So, $u^{-1}(C) = C^d \mod N$. Note that M and C are just dummy labels for how the function and the inverse act (though we often use them to label the plaintext and the ciphertext). For signatures, the concepts of "plaintext" and "ciphertext" are not applicable. We ask you to learn that, to sign, the sender (Ursula) applies the function u^{-1} which is exponentiation with her (the sender's) private key. Note that one signs the same way regardless of who the receiver is.

The last paragraph treats the case when Ursula wishes to both encrypt and sign a message M. Now, we must ask who is the receiver, since the message will be encrypted for him/her. In the book, Sue is the receiver. To help clarify things later, let her public and private keys be (e_j, N_j) and (d_j, N_j), so, Sue's encryption function s is given by $s(H) = H^{e_j} \mod N_j$ (any H is encrypted as $s(H)$).
The book says Ursula sends $s(u^{-1}(M))$. It means Ursula first apply u^{-1} to M, then applies s to $u^{-1}(M)$. That is, Ursula first signs (with her private key) then encrypts (with Sue's public key).
What she sends is $(M^d \pmod N)^{e_j} \mod N_j$.

This last paragraph has 3 problems. First, in most applications, we produce a signature that is appended to the message, but in the book, we simply has a "signed-message". Second, the above procedure only makes sense if $N \leq N_j$. If $N_j < N$, two different initial messages can become congruent mod N_j. (But if $N \leq N_j$, we still have a problem when Sue wants to sign and encrypt a message to Ursula.) The truth is that, if $N > N_j$, we need to re-express $u^{-1}(M)$ (which ranges from 0 to $N-1$) in symbols running from 0 to N_j before applying the encryption step. Third, we never explain why we sign first then encrypt, rather than encrypt then sign. This is out of scope of the textbook, but here're some ideas in simple terms:

Note that encryption involves protection of the sender and the receiver from a curious 3rd party to learn their communications. So, they are trusted when we discuss encryption.
Shifting gear to signatures, we want to keep the sender honest (against repudiation), so we demand something from the sender. In some textbooks, they mention:
• The encrypt-then-sign method is insecure since a dishonest receiver can unsign for the sender and resign in his/her own name. This happens sometimes, say, when someone plagiarizes a photo by removing the correct watermark and add his/her own.
• The sign-then-encrypt method can also be insecure if a dishonest receiver undoes the encryption, and re-encrypts for a different user. The classical example is that Alice can sign "I love you" and encrypts for Bob, who decrypts and reencrypts using Charlie's public key and surreptitiously forward it to Charlie, so that it seems like Alice has sent and encrypted "I love you" to Charlie, which is clearly not so desirable.
Note that these are new insecurities due to the new worry of a dishonest receiver

For the purpose of Ma135, we only want you to understand the 3 steps encryption, decryption and signature, and who does what using which key. You aren't expected to remember the last paragraph concerning simultaneous signature and encryption – if a question is given concerning such, we will give you the instruction such as which one first and how the data may have to be re-expressed in a different modulus.