Introduction to Encryption. Lecture 1.

Chapter 1 of the textbook is an interesting historical account, and worth a read. However the history of the subject is not the focus of this course, so we begin with Chapter 2.

A remark on organization of material:
We'll learn a handful of "ancient" cryptosystems up front, and then learn how to attack them later.
(This, as opposed to the approach of presenting a new system, its weaknesses, and then developing a tougher system in response to those weaknesses).

Our focus will be on <u>valid</u> cryptosystems in history.
We call a system valid if:

① • Messages are easy to encrypt

② • Messages are easy to send

③ • Messages are easy to read if you are the intended recipient

④ • Messages are hard to read if you are <u>not</u> the intended recipient.

⑤ • It should be easy to verify that the message comes from the correct source.