

- BASE! HEADQUARTERS" (b)  $C = AP + B$ ,  $A = \begin{pmatrix} 103 & 30 \\ 10 & 7 \end{pmatrix}$ ,  $B = \begin{pmatrix} 301 \\ 412 \end{pmatrix}$ ; "INJUFYKTEGOUL IB!VFEXU!JHALGQGJ?"
26.  $29^8(29^2 - 1)(29^2 - 29) = 341,208,073,352,438,880$ .
27. 91,617,661,629,000,000.
28.  $A^{-1} = \begin{pmatrix} 18 & 21 & 19 \\ 13 & 18 & 3 \\ 3 & 19 & 11 \end{pmatrix}$ , "SENDROSESANDCAVIARJAMESBOND."

### § IV.1.

1.  $\binom{m}{2} = m(m - 1)/2$  for classical;  $m$  for public key; 499500 versus 1000 when  $m = 1000$ .
2. Here is one possible method. The investors and stockbrokers use a system with  $\mathcal{P} = \mathcal{C}$ . Then user A sends a message to user B by taking each message unit  $P$  and transmitting  $f_B f_A^{-1}(P)$ . Each message includes an identification number. Then user B must immediately send an acknowledgment message which includes the identification number of the message received from A. User B transforms each message unit  $P$  of the acknowledgment message to  $f_A f_B^{-1}(P)$  before transmitting it (this is completely analogous to A's double enciphering of the original message). If A does not receive an acknowledgment message very soon after sending his message, he repeats the message until he does. Later, after the stock loses money or for some reason there is a dispute about who sent what message, the stockbroker can prove that a message was sent by A, because no one except A (and the judge) has the information necessary to produce a message that can be read by applying  $f_A f_B^{-1}$ . Similarly, A can prove that a message with a given identification number was received by B (since no one else could have sent the acknowledgment message), and so B can be required to produce the message for the judge.
3. A public key cryptosystem is agreed upon which uses random integers (subject to some conditions, perhaps) to form enciphering and deciphering keys according to some algorithm. The computer is then programmed to generate random integers which it then uses to form a pair of keys  $K = (K_E, K_D)$ . The computer transmits  $K_D$  (*not*  $K_E$ ) to the outside world and keeps  $K_E$  (*not*  $K_D$ ) to itself. Thus, anyone at all can read its messages, but no one at all can create a message that can be deciphered using the deciphering algorithm with key  $K_D$ . (This is the reverse of the usual situation in public key cryptography, where anyone can send a message but only the user with the secret key can read it.) It is possible for the scientists working jointly to program the computer to generate random numbers in a way that no one can predict or duplicate once the computer is "on its own." (Note the profound realism of this example, which assumes that the two countries have infinite mistrust of each other and at the same time infinite trust of computers.)