

$$\begin{aligned}
\begin{pmatrix} f_{n+b+1} & f_{n+b} \\ f_{n+b} & f_{n+b-1} \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+b} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^b \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \\
&= \begin{pmatrix} f_{b+1} & f_b \\ f_b & f_{b-1} \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \\
&\equiv \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \\
&= \begin{pmatrix} cf_{n+1} & cf_n \\ cf_n & cf_{n-1} \end{pmatrix} \pmod{a},
\end{aligned}$$

where  $c \in (\mathbf{Z}/a\mathbf{Z})^*$ , and use the induction assumption. (It can be proved that for *any* integer  $a$  there is an integer  $b$  such that  $a|f_n \iff b|n$ , and that if  $a = p^\alpha$  is a power of a prime  $p \neq 5$ , then  $b$  is a divisor of  $p^{\alpha-1}(p^2 - 1)$ ; the proof uses a little algebraic number theory in the real quadratic field generated by the golden ratio — note that the golden ratio and its conjugate are the eigenvalues of the matrix in the definition of Fibonacci numbers.)

7.  $A^{-1} = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix}$ , "SENATORTOOK."
8.  $A^{-1} = \begin{pmatrix} 22 & 16 \\ 21 & 17 \end{pmatrix}$ , "MEET AT NOON."
9.  $A^{-1} = \begin{pmatrix} 22 & 20 \\ 28 & 8 \end{pmatrix}$ , "WHY NO GO? MARIA";  $A = \begin{pmatrix} 3 & 7 \\ 4 & 1 \end{pmatrix}$ , "JMLD W EFWJV."
10. "CJIABA KIICC", which is Russian for GLORY TO THE CPSU (Communist Party of the Soviet Union).
11. The product cryptosystem has enciphering matrix  $A_2A_1$ .
12. "?CVK"; first apply  $\begin{pmatrix} 18 & 28 \\ 19 & 20 \end{pmatrix}$  to the ciphertext vector, working modulo 29, and then apply  $\begin{pmatrix} 15 & 15 \\ 22 & 3 \end{pmatrix}$  to the resulting vector, working modulo 26; "STOP."
13. By Proposition 3.2.1 (namely, (b) false implies (c) false), there exists a nonzero vector which the matrix  $A$  takes to  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ . That plaintext digraph-vector can be added to any plaintext digraph-vector without changing the corresponding ciphertext.
14. Here the ciphertext is

$$\begin{pmatrix} 18 & 6 & 11 & 10 & 29 & 14 & 16 & 11 & 14 & 10 & 11 & 21 \\ 26 & 13 & 8 & 3 & 10 & 25 & 11 & 8 & 12 & 20 & 27 & 24 \end{pmatrix}$$

and the last three columns of plaintext are  $\begin{pmatrix} 10 & 17 & 0 \\ 0 & 11 & 27 \end{pmatrix}$ . The determinant of the matrix formed by the first two of the latter three columns is  $20 \pmod{30}$ , which is not invertible modulo 30 but is invertible modulo 3. The determinant of the matrix formed by the second and third columns is  $9 \pmod{30}$ , which is not invertible modulo 30 but