10. (a) $a' = 435$, $b' = 64$; "FOUNDTHEGOLD"; (b) $a = 115$, $b = 76$; "AWOFUWAE."
11. (a) You cannot find the key from the first two congruences; but subtracting the third from the first gives $139a' \equiv 247 \ mod\ 900$, and then $a' = 73$, $b' = 768$; "ARE YOU JOKING?"; (b) $a = 37$, $b = 384$; "FWU ORI DCCUVGA ."
12. "CCCP", which is Russian for USSR.
13. $P \equiv 37P + 384 \ mod\ 900$ leads to $3P \equiv 43 \ mod\ 75$; none.
14. (a) The product of $I \equiv P + b_1 \ mod\ N$ and $C \equiv I + b_2 \ mod\ N$ is $C \equiv P + b \ mod\ N$ with $b = b_1 + b_2$. (b) The product is the linear transformation with $a = a_1 \cdot a_2$. (c) The product is the affine transformation with $a = a_1 \cdot a_2$ and $b = a_2 \cdot b_1 + b_2$.
15. $P \equiv 642C + 187 \ mod\ 853$; "DUMB IDEA ."
16. First compute $I \equiv 201C + 250 \ mod\ 881$ and then $P \equiv 331I + 257 \ mod\ 757$; "NO RETREAT."

**§ III.2.**

1. The key-word for enciphering is "SPY." The plaintext (with blanks and punctuation inserted for readability) is: "I had asked that a cable from Washington to New Delhi summarizing the results of the aid consortium be repeated to me through the Toronto Consulate. It arrived in code; no facilities existed for decoding. They brought it to me at the airport — a mass of numbers. I asked if they assumed I could read it. They said no. I asked how they managed. They said when something arrived in code, they phoned Washington and had the original message read to them." (John Kenneth Galbraith, *Ambassador's Journal*, quoted by G. E. Mellen in "Cryptology, computers and common sense," vol. III of *Computers and Security*.)
2. (a) $\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$; (b) $\begin{pmatrix} 19 & 10 \\ 23 & 16 \end{pmatrix}$; (c) $\begin{pmatrix} 11 & 11 \\ 24 & 1 \end{pmatrix}$; (d) $\begin{pmatrix} 820 & 0 \\ 0 & 801 \end{pmatrix}$; (e) $\begin{pmatrix} 127 & 303 \\ 546 & 353 \end{pmatrix}$.
3. (a) $\binom{6}{1}$; (b) none (since multiplying the second congruence by 2 and subtracting from the first gives $6y \equiv 8 \ mod\ 9$, which would mean $3|8$); (c) $\binom{6}{1}$, $\binom{3}{4}$, $\binom{0}{7}$; (d) $\binom{0}{0}$, $\binom{6}{3}$, $\binom{3}{6}$.
4. (a) $\binom{9}{21}$; (b) $\binom{0}{0}$; (c) any vector with $y = x$, i.e., $\binom{0}{0}$, $\binom{1}{1}$, $\binom{2}{2}$, etc.; (d) any vector of the form $\binom{n}{15+n}$; (e) none.
5. (a) $\binom{787}{759}$; (b) $\binom{626}{233}$; (c) $\binom{0}{0}$; (d) $\binom{0}{0}$, $\binom{101}{505}$, $\binom{202}{1010}$, $\binom{303}{404}$, $\binom{404}{909}$, $\binom{505}{303}$, $\binom{606}{808}$, $\binom{707}{202}$, $\binom{808}{707}$, $\binom{909}{101}$, $\binom{1010}{606}$; (e) add $\binom{31}{800}$ to any of the 11 vectors in part (d) and reduce mod 1111.
6. Use mathematical induction, proving the assertion for $n = 1, 2, \ldots, b$ by inspection and then proving that the assertion for $n$ implies the assertion for $n + b$. Namely, compute: