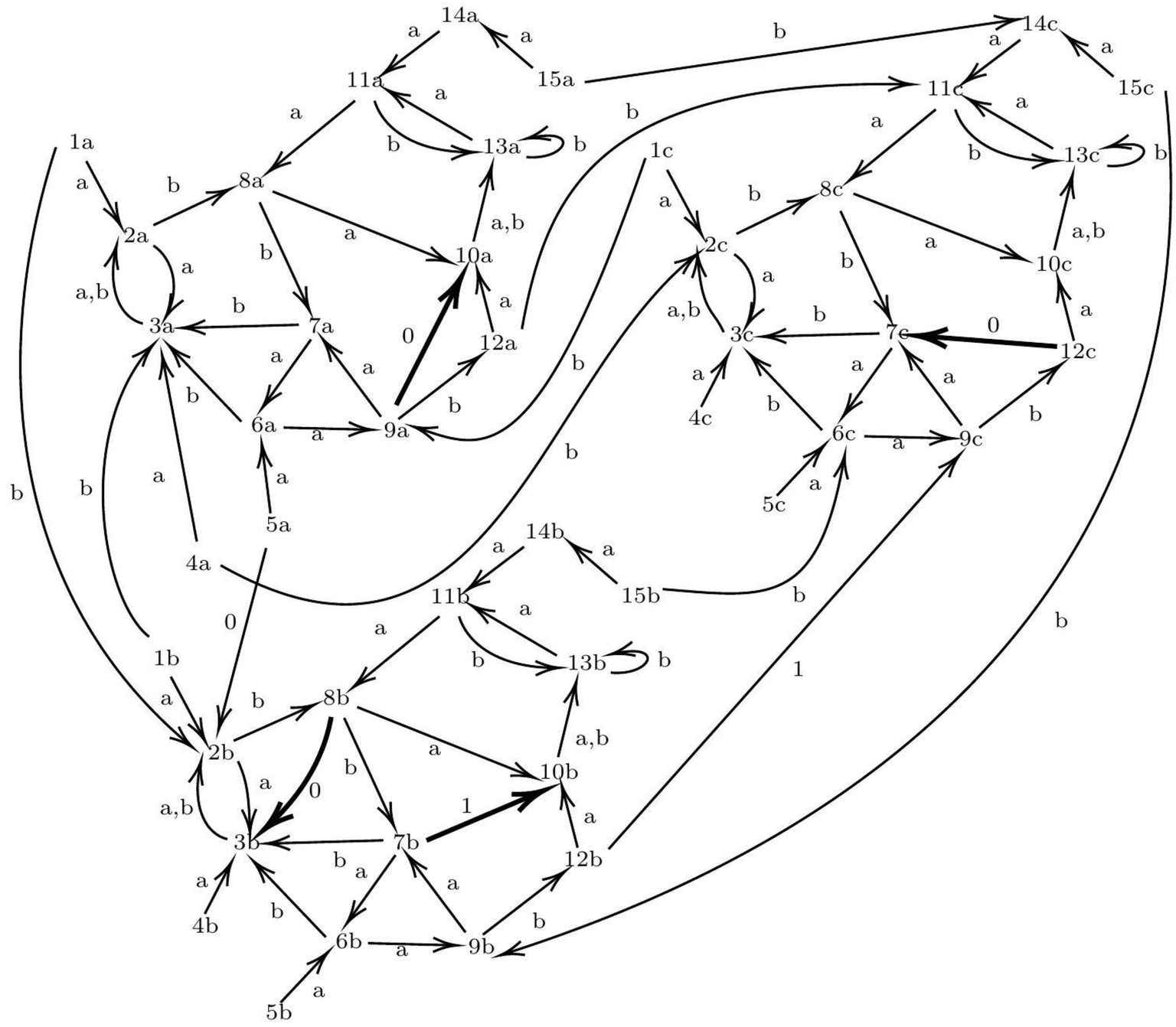

Figure 6: Fourth step of encryption.

The last step involves adding some number of transitions under letters from the alphabet $\{0, 1\}$ between states belonging to the same copy of a public key in $\mathcal{B}$. In that case we have added transition $\rho(9a, 0) = 10a$ (first copy), transitions $\rho(7b, 1) = 10b$ and $\rho(8b, 1) = 3b$ (second copy) and transition $\rho(12c, 0) = 7c$ (third copy).

4 Basic decryption

For that section we assume that we have a ciphertext automaton $\mathcal{B} = (P, \Sigma, \rho)$ constructed from a public key $\mathcal{A} = (Q, \Sigma, \delta)$, and that we know a private key w which is a carefully synchronizing word for the automaton $\mathcal{A}$. First we state a lemma.

Lemma 1. *Let $Q.w = q_l$. After removing letters $x \in \{0, 1\}$ from automaton $\mathcal{B}$ we have that $P.w = \{q_l^1, q_l^2, .., q_l^{|u|+1}\}$.*