Οι ιδέες που χρησιμοποίησα είναι:

α) Αντικατάσταση με ένα κλειδί

β) Αλλαγή με δύο κλειδιά

γ) Αλλαγή με τρία κλειδιά

δ) Αντικατάσταση με ένα κλειδί και μετά transposition

Για την αποκρυπτογράφηση του puzzle 5, έχω δοκιμάσει όλους τους πιθανούς συνδυασμούς ενός κλειδιού 7 ψηφίων (καθώς οι ταυτότητες είναι 5 έως 7 κλειδιά). Η Αλίκη χρησιμοποίησε την ταυτότητά της στο πανεπιστήμιο, οπότε μάντεψα ότι χρησιμοποίησε τον αριθμό ταυτότητάς της. Δοκίμασα με ωμή βία όλους τους πιθανούς αριθμούς ταυτότητας και το βρήκα.

Πιστεύω ότι η πρακτική της Αλίκης να χρησιμοποιεί την ταυτότητά της δεν είναι έξυπνη, γιατί κάποιος μπορεί να μαντέψει το κλειδί. Ο αλγόριθμος AES 128 bit μπορεί να χρησιμοποιήσει οποιοδήποτε κλειδί 128 bit, το οποίο μπορεί να μην έχει συνδυασμό γραμμάτων, συμβόλων, κεφαλαίων γραμμάτων κ.λπ. Αυτό δεν διευκολύνει απαραίτητα το σπάσιμο του αλγόριθμου, γιατί αν θέλουμε πραγματικά να αναγκάσουμε τους χρήστες να χρησιμοποιήσουν καλύτερο κωδικό πρόσβασης, μπορούμε να το κάνουμε σε επίπεδο λογισμικού (να ελέγχετε ο κωδικός πρόσβασης πριν να χρησιμοποιηθεί πραγματικά).