1 M-138-A

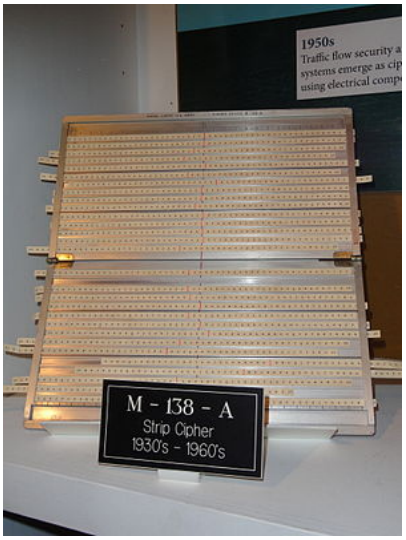

Рис. 1: M-138-A

M-138-A является низкотехнологичным шифровальным устройством первой половины 20-го века. Несмотря на то, что M-138-A довольно прост, его трудно сломать. M-138-A (также известный как CSP-845) - это шифровальная система, основанная на полиалфавитном шифровании. M-138-A была введенна Вооруженными силами США в 1930-х годах. Цель м-138-A заключалась в обеспечении средней безопасности при низких затратах. Он использовался, когда шифровальная машина (например, M-209 или SIGABA) была недоступна. Это случалось довольно часто, так как шифровальные машины были на порядок дороже ленточных шифров и сложнее в транспортировке.

До и в начале Второй мировой войны большое внимание уделялось м-138-A из-за нехватки шифровальных машин. Позже он остался в использовании в качестве резервной системы для шифрования

1.1 Как работает M-138-A

M-138 состоит из 100 бумажных полосок, на каждой из которых алфавит печатается дважды в случайном порядке. Для шифрования шифровальщик должен был взять некоторо количество полосок и поместить их в кадр шифровального устройства.

В нулевом(или в первом) столбце должно быть записано исходное сообщение. А столбец с шифротекстом Вы выбираете самостоятельно.

В следующем примере полосы 66, 11, 52, 55, 04 и 90 выбраны для шифрования слова CRYPTO.

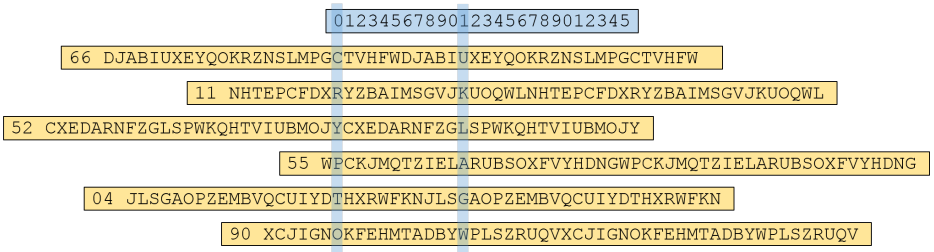

Рис. 2: Пример

Ключ этой процедуры шифрования (66, 11, 52, 55, 04, 90 / 11). Он состоит из полосовых номеров, используемых с последующим смещением исходного текста и столбцом шифротекста. В этом примере зашифрованным текстом является UKLAGW.

А если бы мы выбрали второй столбец, то ключ был бы (66, 11, 52, 55, 04, 90 / 2), а шифротекст - TYCCHK.