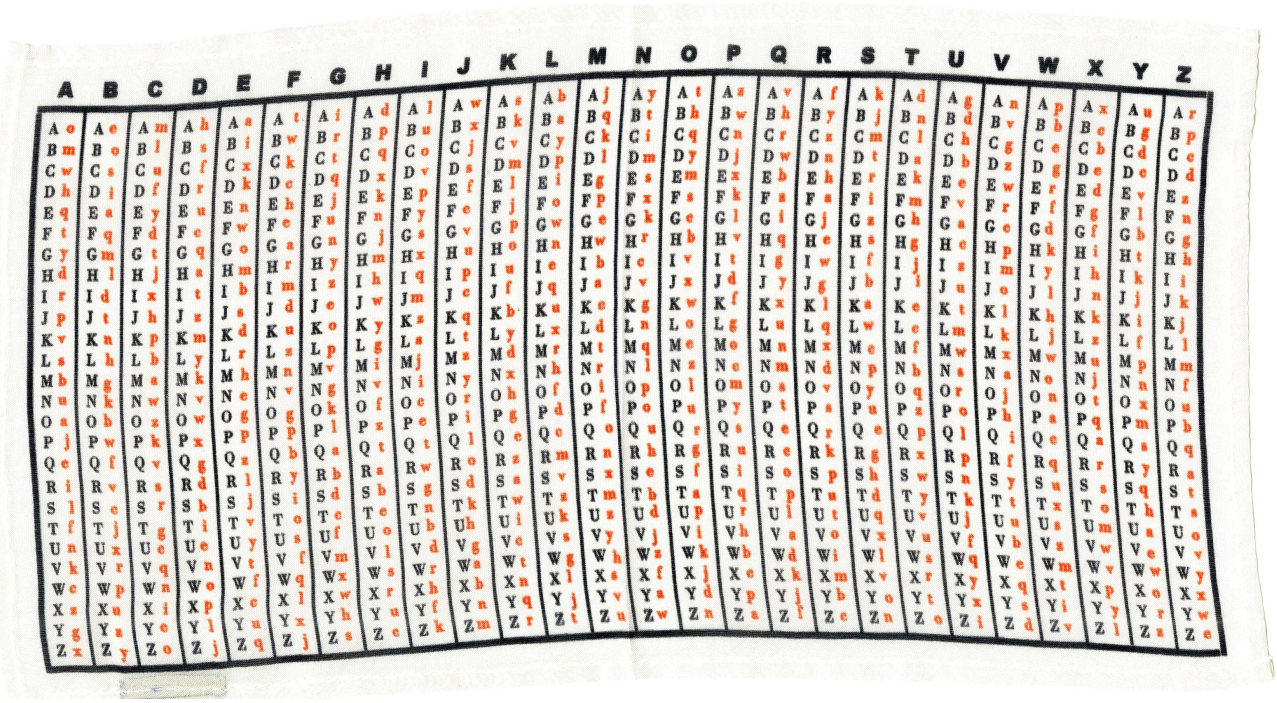
Association des Anciens Combattants
Services de Renseignement de France et des Pays Alliés
<< EX-INVISIBLES (A.C.S.R.) >>

Un codage de messages

Par Daniel TANT

Voici un système astucieux nommé « one-time-pad », utilisé pendant la Seconde guerre mondiale. Chaque lettre d'un message en clair pouvait être codé par plusieurs possibilités. Imaginons le codage du mot « indivisibilité ». Si nous prenons la verticale « D » et que nous descendons jusqu'à la lettre « T », nous obtenons un premier « I ». Si nous prenons la colonne « R » et que nous descendons jusqu'à « D », nous obtenons « N ». Avec la colonne « I » jusqu'au « V », nous obtenons « D ». « Indivisibilité » codé sera, par exemple, DT – RD – IV – XH – DN – UZ – CR – BD – NT – FS – VK – GA – MM – IP. Remarquons qu'une même lettre peut être codée de 26 façons différentes ce qui évite au « cabinet noir » ennemi de décrypter le message.