Définition. GCM (Galois Counter Mode).

Soient $e(.)$ un B-cryptage de taille 128 bits;

x le clair $= (x_1, \dots, x_n)$

AAD = additional authenticated data.
(ex. nom, fonction, mail, etc)

1. **Cryptage**
   a. Déduire une valeur CTR_0 de IV et calculer
   $$CTR_1 = CTR_0 + 1.$$
   b. Calculer les chiffrés $y_i = e_k(CTR_i) \oplus x_i$, $i \geq 1$.

2. **Authentification**
   a. Générer une sous-clé d'authentification $H = e_k(0)$.
   b. $g_0 = AAD \times H$
   c. $g_i = (g_{i-1} \oplus y_i) \times H \quad (1 \leq i \leq n)$
   d. Calculer le ~~tag~~ $T = (g_n \times H) \oplus e_k(CTR_0)$.

- Bob reçoit $[(y_1, \dots, y_n), T, ADD]$ et calcule $(x_1, \dots, x_n)$ avec la même procédure en mode CTR. Ensuite, avec l'algorithme GCM calcule T' en utilisant (y_i) et ADD. Si $T = T'$, alors Bob est sûr que x et ADD n'ont pas été modifié.
- Tous les calculs sont faits dans $GF(2^{128})$ avec le polynôme irréductible $p(x) = x^{128} + x^7 + x^2 + x + 1$.