# Connexion sécurisée HTTPS

## Protocole Transport Layer Security (TLS)

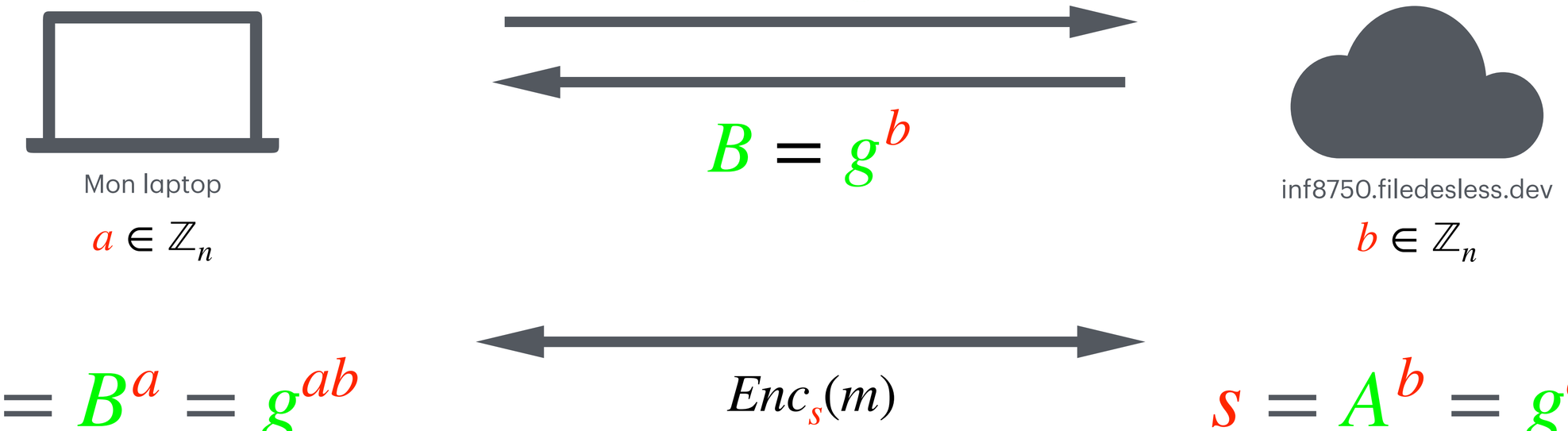

En détails: https://tls13.xargs.org/

# Établissement de clé

## Algorithme de Diffie-Hellman général

$g$: générateur fixé d'un groupe cyclique

Hypothèse de sécurité: logarithme discret




$(a, A)$: clé de session du client

$s$: clé de session partagée

$(b, B)$: clé de session du serveur