# Application de messagerie instantanée

# Contexte

Alice et Bob veulent communiquer par un système de messagerie instantané.
Ce système doit fournir les propriétés de sécurité suivantes

# Contexte

Alice et Bob veulent communiquer par un système de messagerie instantané.
Ce système doit fournir les propriétés de sécurité suivantes

- Authentification des différents partis (ici Alice et Bob)

# Contexte

Alice et Bob veulent communiquer par un système de messagerie instantané.
Ce système doit fournir les propriétés de sécurité suivantes

- Authentification des différents partis (ici Alice et Bob)
- Mode Asynchrone: communication « offline » possible

# Contexte

Alice et Bob veulent communiquer par un système de messagerie instantané.
Ce système doit fournir les propriétés de sécurité suivantes

- Authentification des différents partis (ici Alice et Bob)
- Mode Asynchrone: communication « offline » possible
- Chiffrement des échanges

# Contexte

Alice et Bob veulent communiquer par un système de messagerie instantané.
Ce système doit fournir les propriétés de sécurité suivantes

- Authentification des différents partis (ici Alice et Bob)
- Mode Asynchrone: communication « offline » possible
- Chiffrement des échanges
- Intégrité des données transmises

# Contexte

Alice et Bob veulent communiquer par un système de messagerie instantané.
Ce système doit fournir les propriétés de sécurité suivantes

- Authentification des différents partis (ici Alice et Bob)
- Mode Asynchrone: communication « offline » possible
- Chiffrement des échanges
- Intégrité des données transmises
- Protection contre les attaques par rejeu

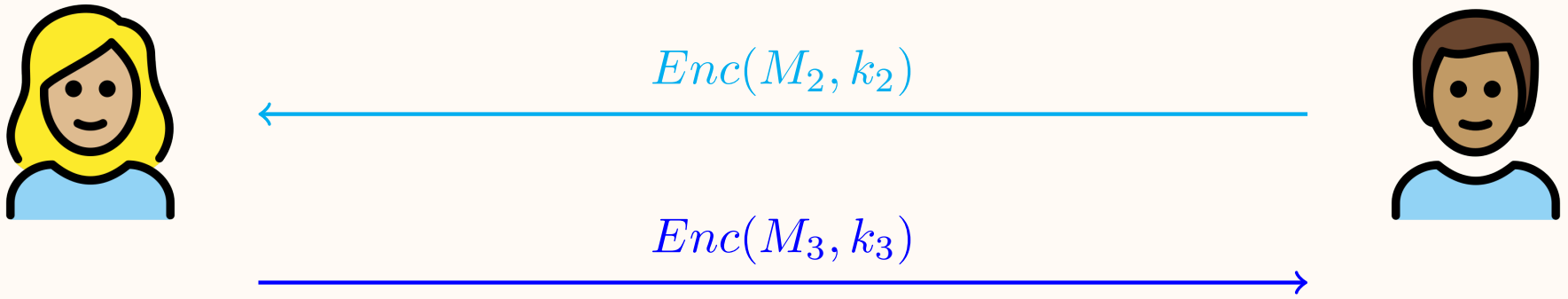
# Contexte

Alice et Bob veulent communiquer par un système de messagerie instantané.
Ce système doit fournir les propriétés de sécurité suivantes

- Authentification des différents partis (ici Alice et Bob)
- Mode Asynchrone: communication « offline » possible
- Chiffrement des échanges
- Intégrité des données transmises
- Protection contre les attaques par rejeu
- Sécurité en avant et en arrière

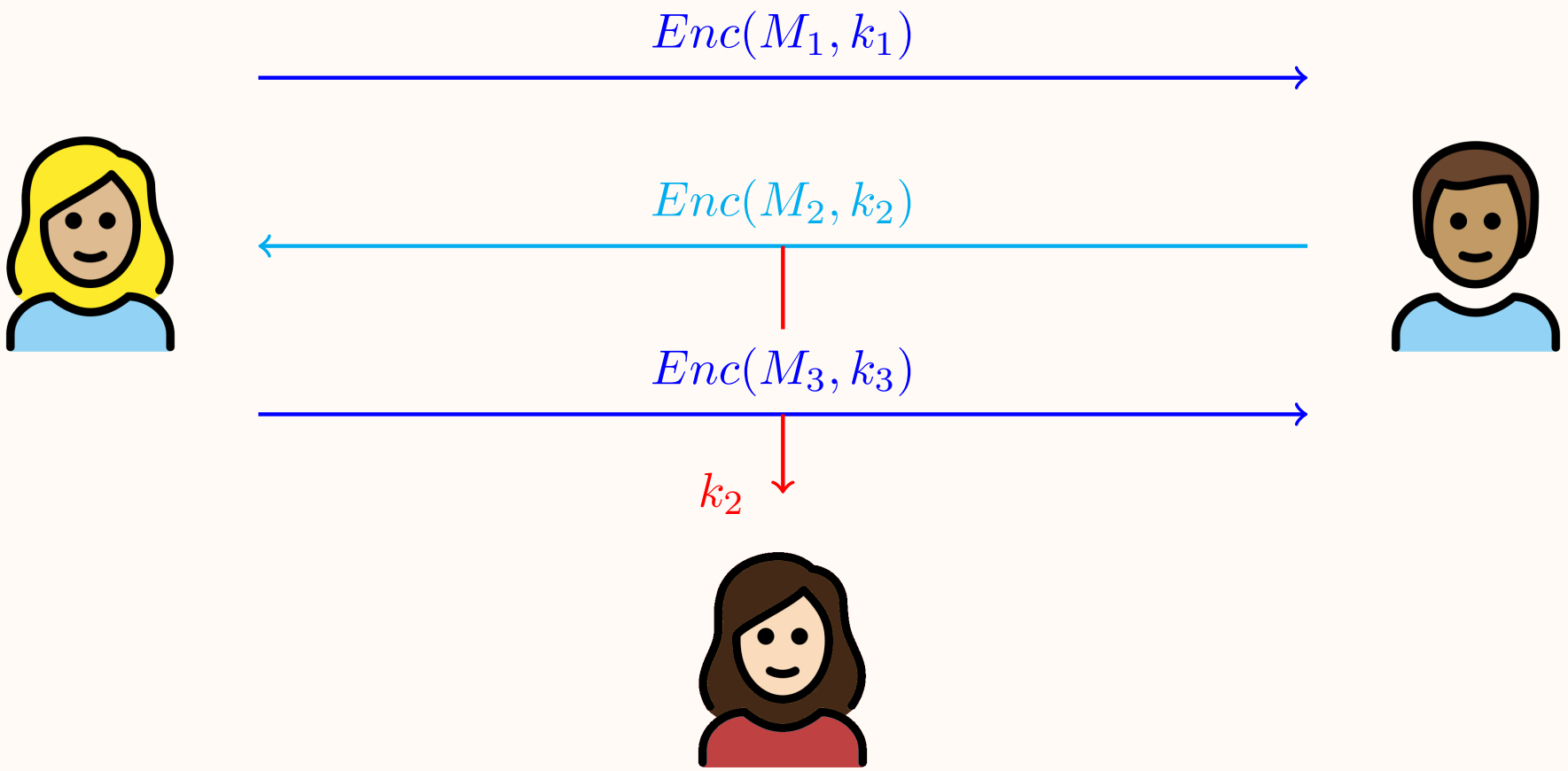
# Sécurité en avant (Forward secrecy)

Aussi appelée confidentialité persistante



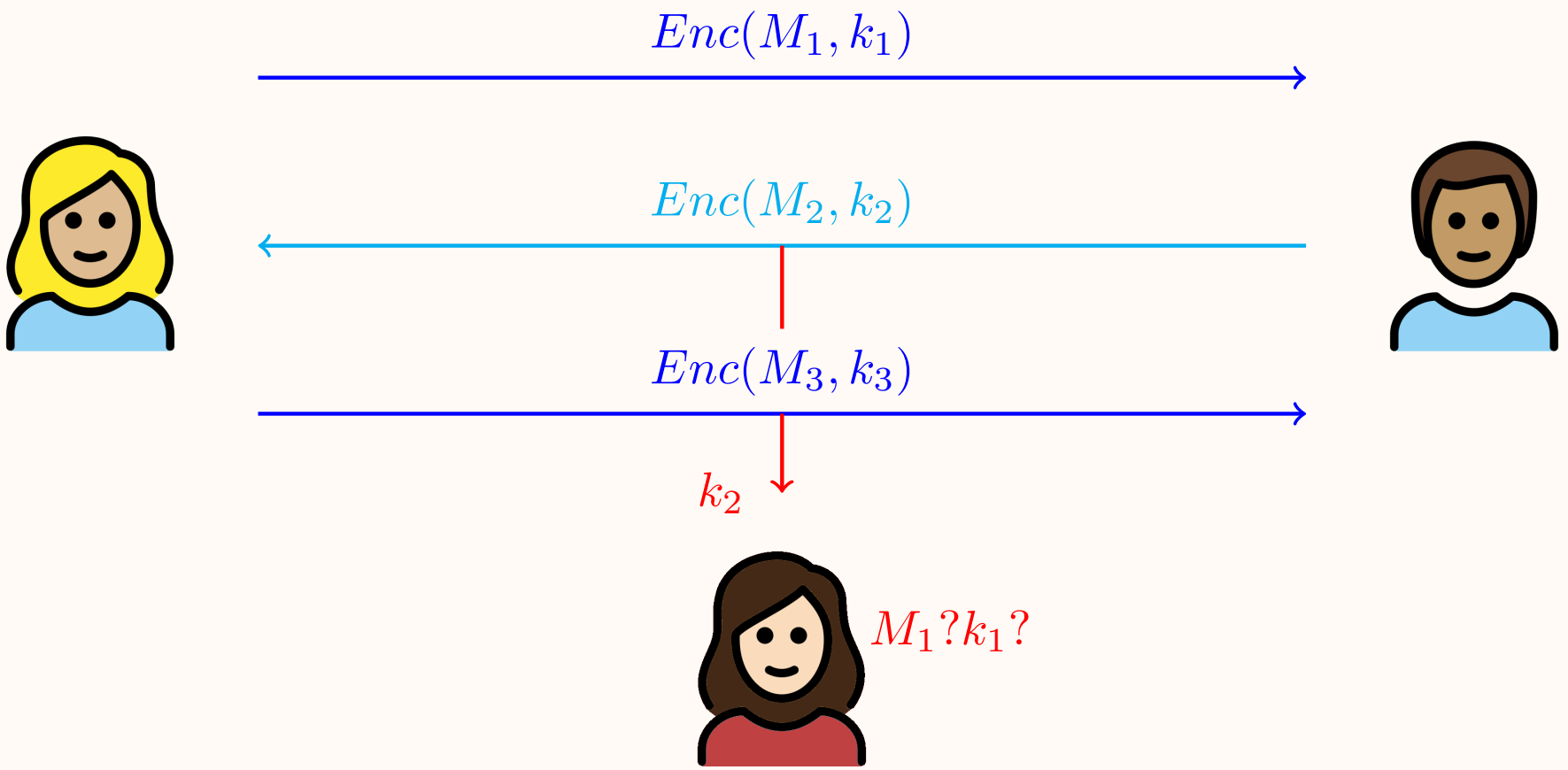
# Sécurité en avant (Forward secrecy)

Aussi appelée confidentialité persistante



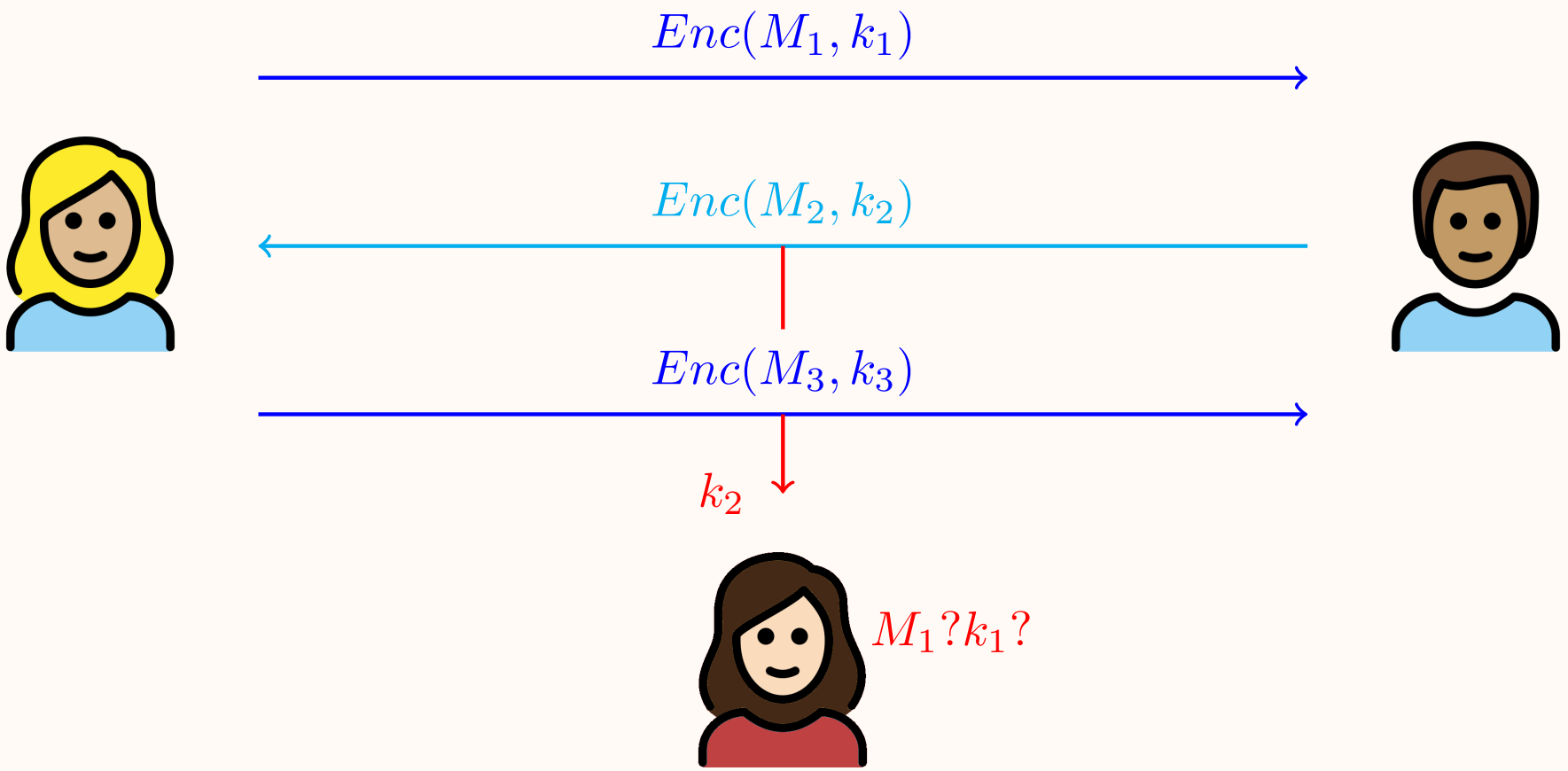
# Sécurité en avant (Forward secrecy)

Aussi appelée confidentialité persistante



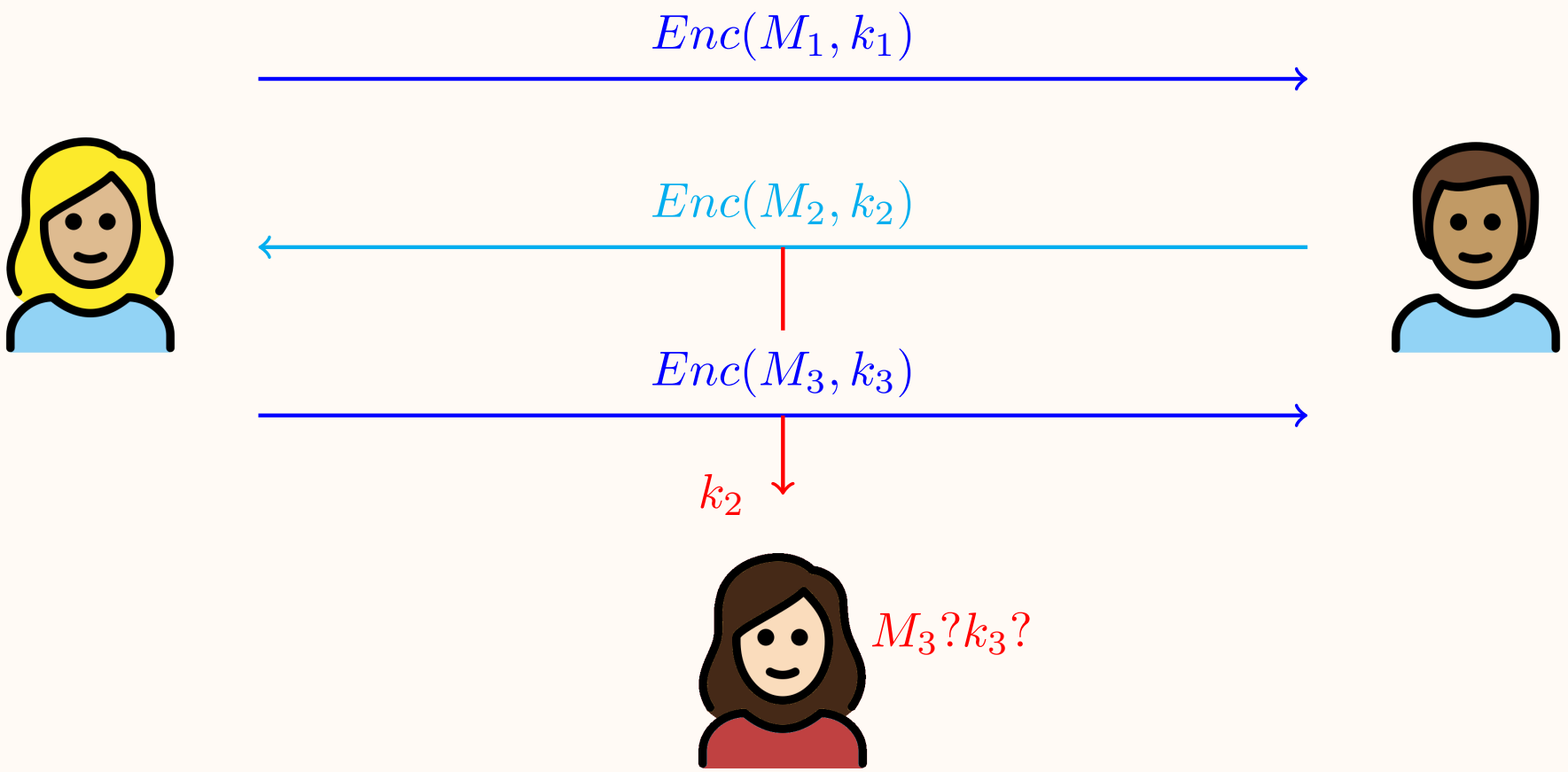
# Sécurité en avant (Forward secrecy)

Aussi appelée confidentialité persistante

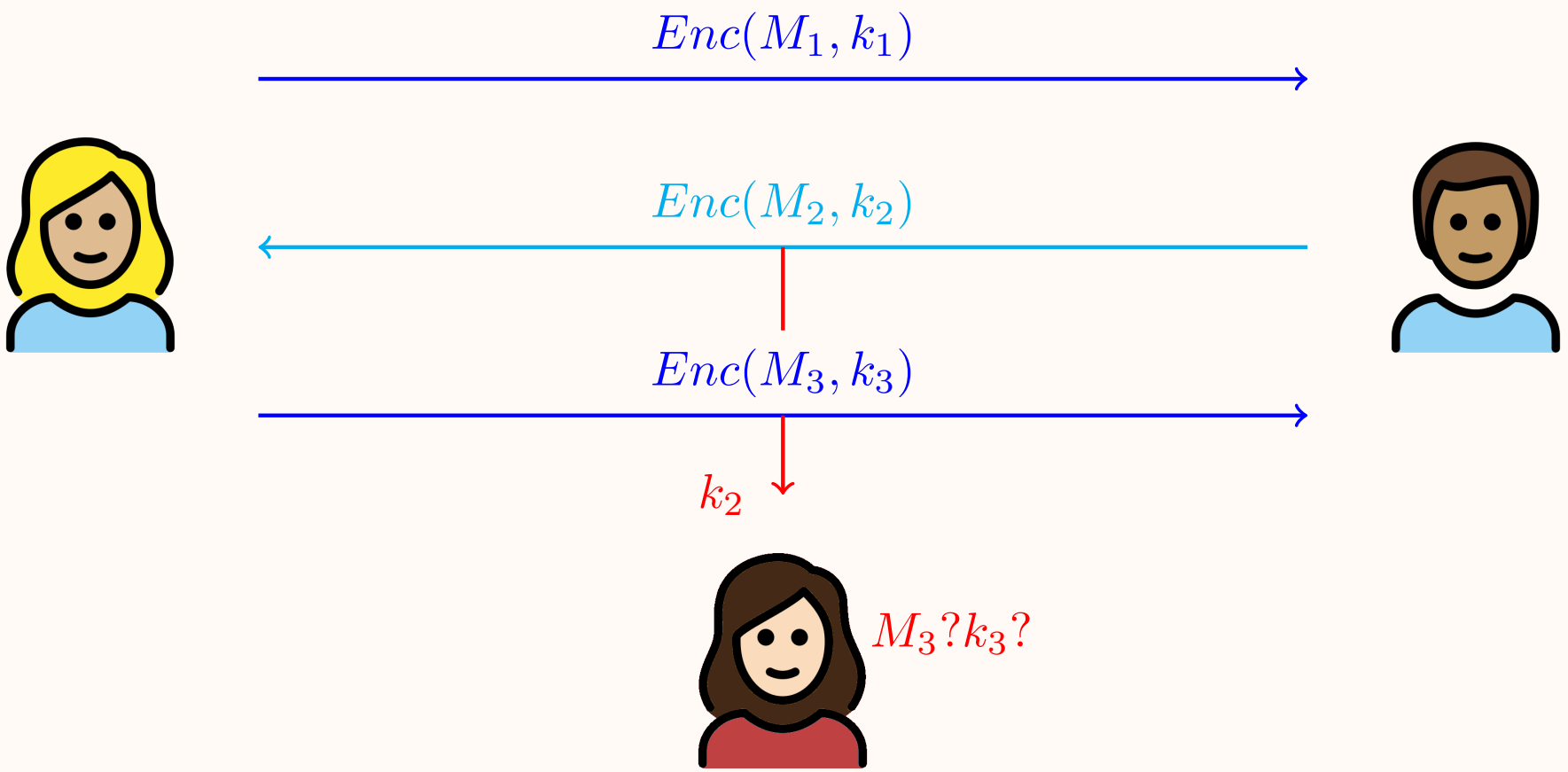



Même en connaissant la clé d'un message $t$, Eve ne peut pas déchiffrer les communications précédentes.

# Sécurité en arrière (Backward secrecy)



# Sécurité en arrière (Backward secrecy)




Même en connaissant la clé d'un message $t$, Eve ne peut pas déchiffrer les communications suivantes.

# Autre pistes à explorer

- Que se passe-t-il si la clé privée d'Alice ou Bob se trouve compromise?
- Comment Alice et Bob peuvent inviter Charlie (et d'autres) à se joindre à la discussion?