

Privacy and End-to-End Encryption

Embedded Ethics Lecture

Veronica A. Rivera, PhD

varivera@stanford.edu



Stanford University
Human-Centered
Artificial Intelligence

Stanford | McCoy Family Center for
Ethics in Society

Today:

Encryption can be used to protect privacy

If we use it well

Privacy in the digital age refers to...

Information



Photo by [Markus Spiske](#) on [Unsplash](#)

Communication



Photo by [freestocks](#) on [Unsplash](#)

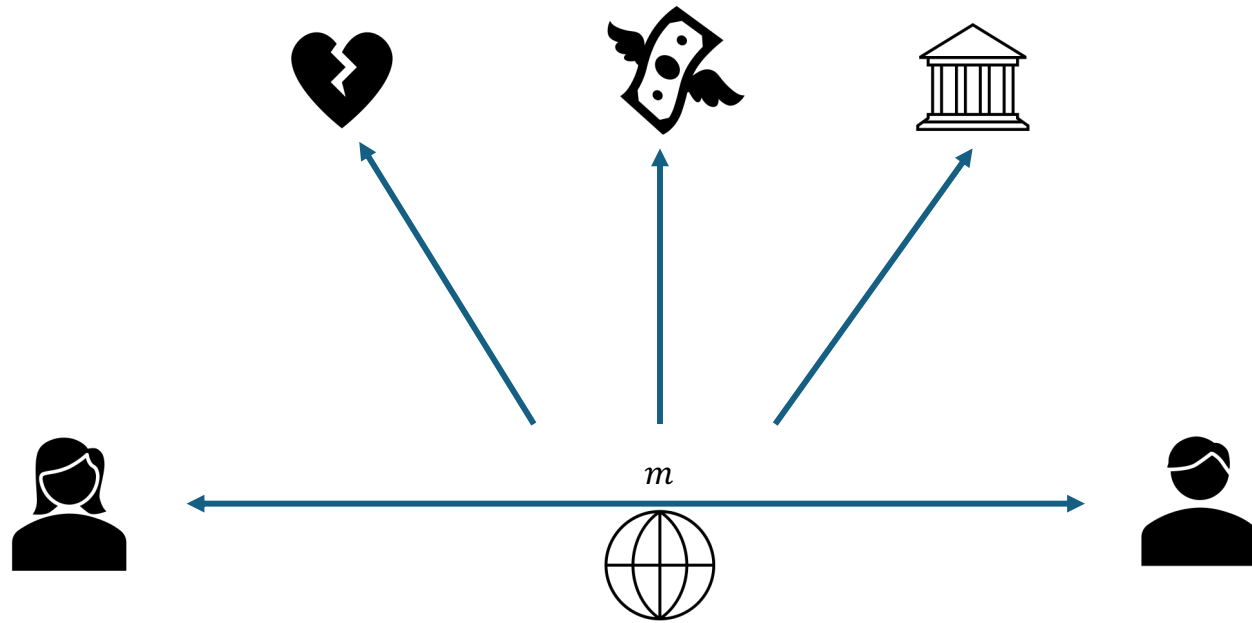
Personal



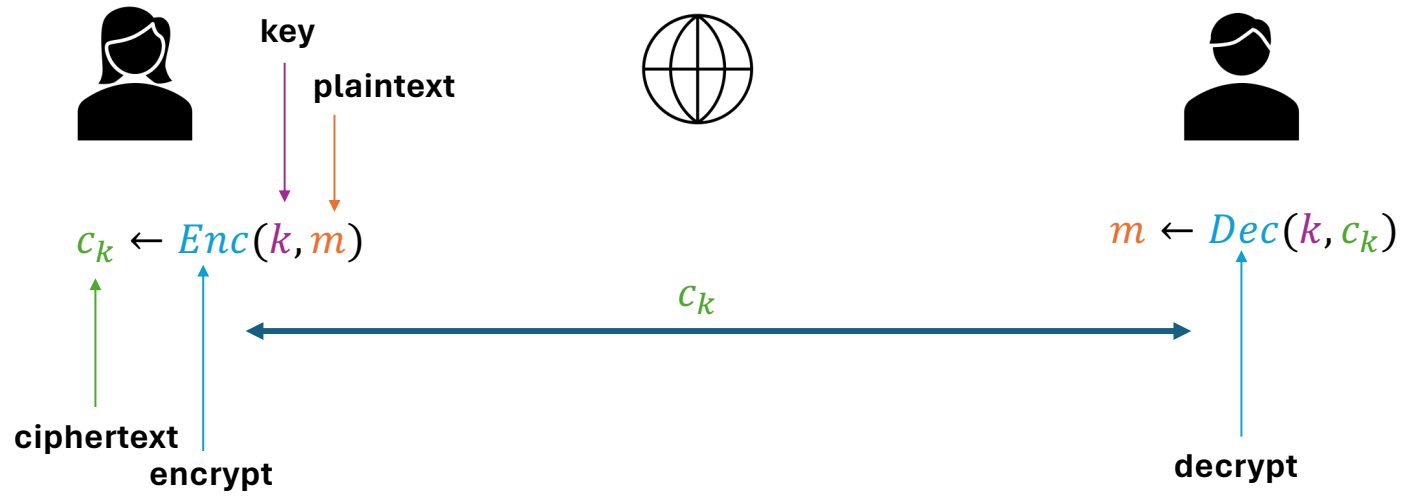
Photo by [bruce mars](#) on [Unsplash](#)

Today

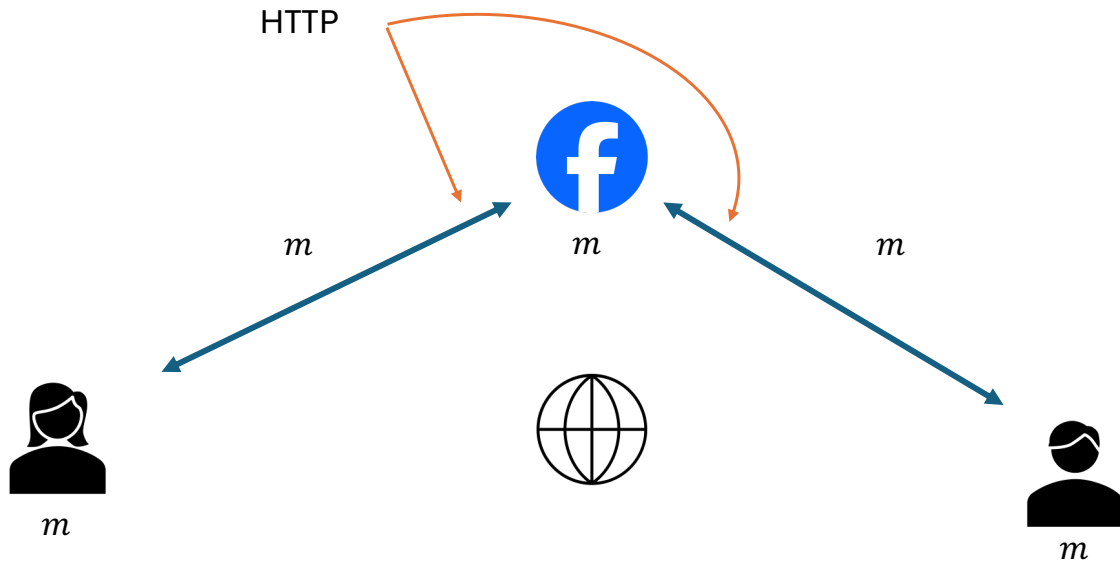
Private messaging is important for daily life



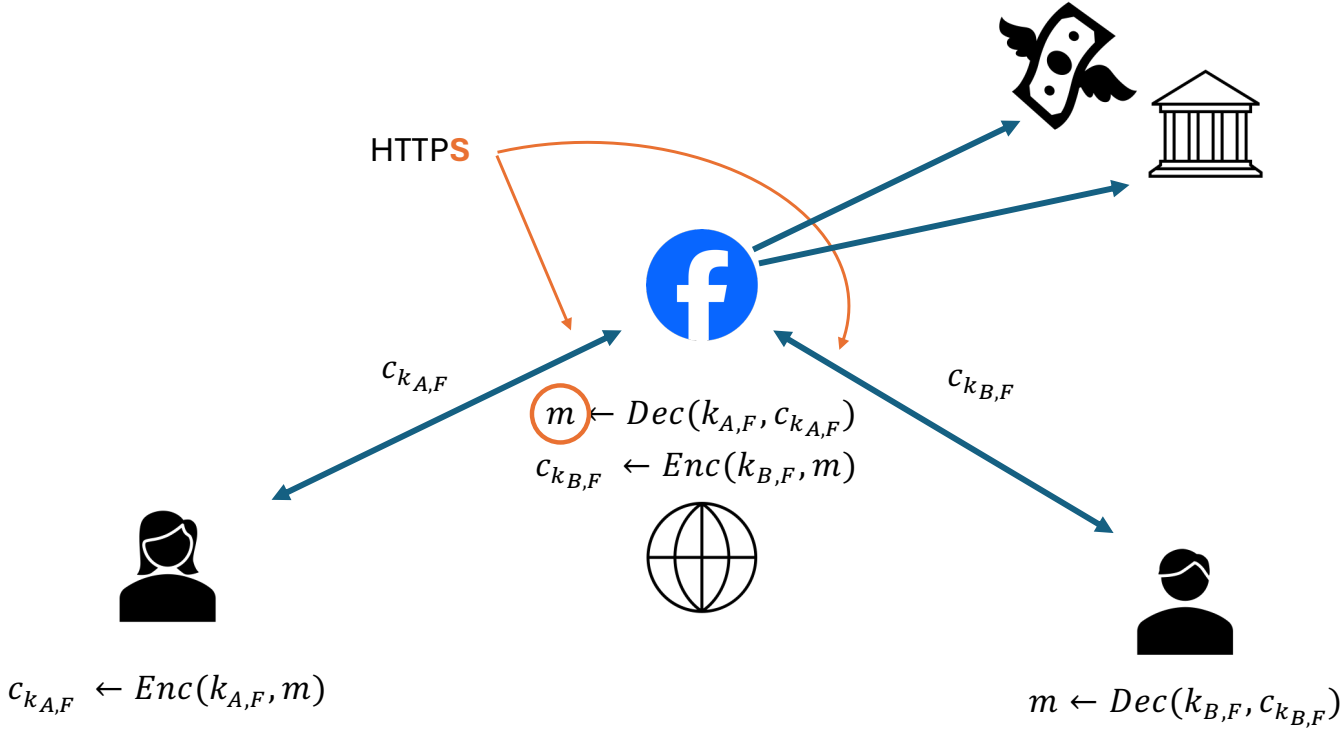
Encryption



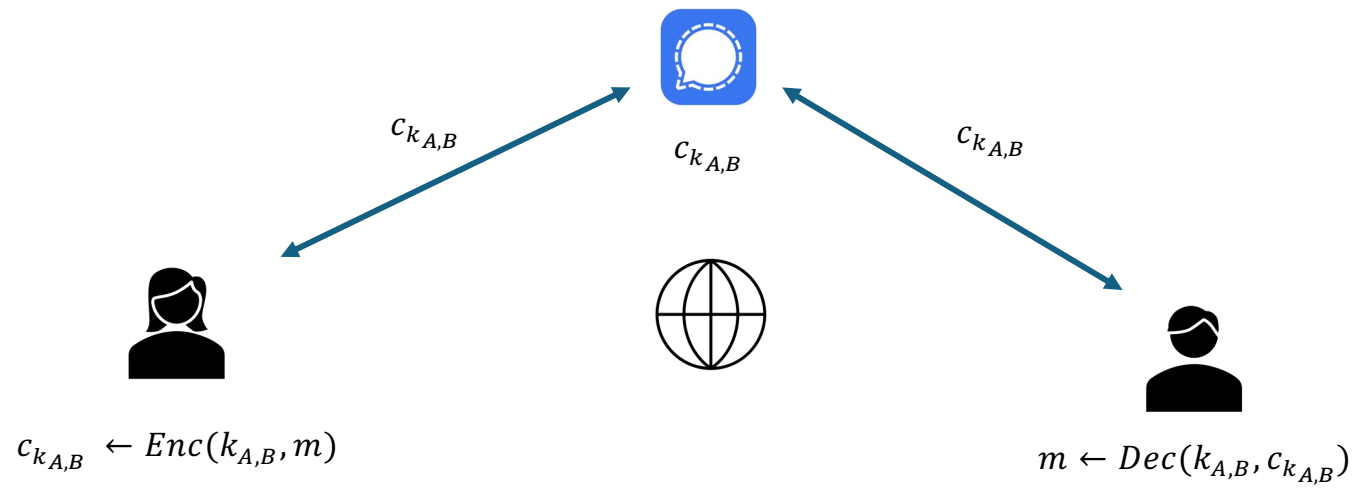
No Encryption (FB 2010)



Transport Layer Security (TLS) (FB 2012): Encryption between clients & servers



End-to-End Encryption



E2EE does not solve all privacy problems

- Need to get random people to agree on shared keys
- Metadata (call logs, phone number, location) isn't hidden and could still be collected
- Content moderation becomes very hard to solve because platform can't read content
- Ends (e.g., phones) are still vulnerable