Today

Encrypted communication

Private communiction

Technology and society

Encrypted communications

Diffie-Hellman

Middleperson detection

Digital signatures

Encryption

$$A \rightarrow B : \alpha^{X_A} \pmod{q}$$
$$B \rightarrow A : \alpha^{X_M} \pmod{q}$$
$$A \rightarrow B : \{k_{AB}\}_{K_A^{-1}}$$
$$B \rightarrow A : \{k_{AB}\}_{K_B^{-1}}$$
$$A \rightarrow B : \left\{\{M_A\}_{K_A^{-1}}\right\}_{k_{AB}}$$
$$B \rightarrow A : \left\{\{M_B\}_{K_B^{-1}}\right\}_{k_{AB}}$$
$$A \rightarrow B : \ldots$$

If someone asked you to design a protocol for secure communication between two endpoints, it might look something like this. This protocol applies cryptographic primitives that we've learned about in various sensible ways, including:

- Diffie-Hellman key agreement ensures that Alice and Bob can generate a key that even a Dolev-Yao attacker can't crack — unless they act as a middleperson
- signing the symmetric key used by both parties will detect a middleperson if it's occurring, assuming Alice and Bob can know each other's public keys
- signing (or MAC'ing) all messages allows Alice and Bob to attest to who write them
- encrypting the signed (or MAC'ed) messages hides their contents from any network observer

Encrypted communications

This gives us:

Confidentiality

Integrity

... the end of protocols?

$$A \rightarrow B : \alpha^{X_A} \pmod q$$
$$B \rightarrow A : \alpha^{X_M} \pmod q$$
$$A \rightarrow B : \{k_{AB}\}_{K_A^{-1}}$$
$$B \rightarrow A : \{k_{AB}\}_{K_B^{-1}}$$
$$A \rightarrow B : \left\{\{M_A\}_{K_A^{-1}}\right\}_{k_{AB}}$$
$$B \rightarrow A : \left\{\{M_B\}_{K_B^{-1}}\right\}_{k_{AB}}$$
$$A \rightarrow B : \ldots$$

Q: ____

So is this it? Do all protocols now follow this basic model? Some thought they would, but ___________________________________?

Communications integrity

What do we want when we talk about integrity?

- **Contracts:** *non-repudiability*
  - Alice can't claim she didn't seal this engineering drawing
  - Bob can *forever* prove that Alice's private key signed it
- **Personal communication:** *authenticity*
  - Alice knows it was Bob who just said X ... *right now*

Digital signatures

Strong integrity

Strong non-repudiation

- ... even several years down the road
- ... even after Bob loses his laptop
- ... then someone can *prove* what Alice said to Bob (**privately!?**)

Digital signatures were designed with one set of constraints in mind, and they work really well for that use case. They do provide ______________________________ assuming that __________ ____.

Digital signatures provide this integrity by providing non-repudiation. This is great for _____________________________, where _________________________, but that's not always what we want!

Privacy and security

Lots of overlap in:

- tools
- techniques
- technologists

Privacy requires security… but not synonymous

People often describe themselves as working in "privacy and security", because they are closely-related fields that are built on many of the same fundamental technologies. Cryptography can be used to help secure a company's intellectual property; it can also be used to help secure my private communincations. These two objectives have many overlapping objectives (confidentiality and integrity on behalf of a user or set of users), but they also have important differences.

You can't have electronic privacy without security: if your systems are vulnerable to your adversaries, they can compromise your privacy by breaking in and stealing (or manipulating!) your systems and information.

Private communication

Only Alice and Bob can read each other's messages

- **confidentiality** — not just in the moment!
- even if Eve acquires k_{AB}, we'd like to minimize the harm done: *perfect forward secrecy*
- Alice doesn't want to depend on Bob for her privacy: *repudiability* — this has implications for **integrity** regime

We don't just want to have our messages be private right now. Even if an attacker manages to "break into" our communication at time t_n, we would like all communications from t_0 to t_{n-1} to remain confidential. That seems like a stretch, but ____________________________.

Unlike many security regimes, privacy often demands _____________________. You can violate my trust by repeating something that I told you in confidence, but it's a whole other level of violation when you record and can ______________ what I said.

Off-the-record (OTR)†

Use short-lived symmetric *session keys*

Compromising Bob's computer provides no help decrypting messages: *perfect forward secrecy*

Use symmetric MACs rather than signatures

"Either Bob said this or I did": *repudiability*

† Borisov, Goldberg and Brewer, "Off-the-record communication, or, why not to use PGP", in *WPES '04: Proceedings of 2004 ACM Workshop on Privacy in the Electronic Society*, 2004. DOI: 10.1145/1029179.1029200. Also see: https://otr.cypherpunks.ca.

We explicitly *want* to be able to repudiate messages. Using symmetric MACs helps with this. Suppose I wanted to prove to someone else that you said something (message M). Using a protocol with digital signatures:

$$A \rightarrow B : \left\{ \{M\}_A^{-1} \right\}_{k_{AB}}$$

Bob could take message $\{M\}_A^{-1}$ and show it to someone else. "See? Here's proof that Alice said M!" If, however, Alice sends $\mathrm{MAC}_{k_{AB}}(M)$ to Bob, Bob can only prove that ________________ ________________________________. Since there are ________________________________, this adds no evidence beyond Bob's say-so that Alice actually said M!

OTR protocol

Broad strokes:

1. Authenticated key exchange (AKE)
2. Message exchanges
3. Frequent *re-keying*

We'll focus on the initial version of the protocol as described in the original paper. This leaves out some of the details that are required to actually implement something that works (e.g., message IDs and key IDs to help Alice and Bob keep track of the communication), but it contains the core ideas. The most recent, detailed version of the protocol can be found at https://otr.cypherpunks.ca/Protocol-v3-4.1.1.html.

OTR message encryption

Diffie-Hellman key exchange

Symmetric-key encryption

Re-key *every message*

If k_{ij} exposed, Eve gets **one message**.

$$A \rightarrow B : g^{x_1}$$
$$B \rightarrow A : g^{y_1}$$
$$A \rightarrow B : g^{x_2}, \{M_1\}_{k_{11}}$$
$$B \rightarrow A : g^{y_2}, \{M_2\}_{k_{21}}$$
$$A \rightarrow B : g^{x_3}, \{M_3\}_{k_{22}}$$

where:

$$k_{ij} = h\left(g^{x_i y_j}\right)$$

Is there anything missing from the protocol as shown on this slide?

Every message adds a ______________________________________, so we ____.

OTR authentication

How does Alice know she's talking to Bob?

The **one** place for digital signatures: authenticating with long-term public keys to detect middleperson / impersonation.

$$A \rightarrow B : \{g^{x_1}\}_{K_A^{-1}}, K_A$$
$$B \rightarrow A : \{g^{y_1}\}_{K_B^{-1}}, K_B$$

Then MACs:

$$A \rightarrow B : g^{x_i+1}, \{M_n\}_{k_{ij}}, \mathrm{MAC}_{h(k_{ij})}\left(\left\{g^{x_i+1}, \{M_n\}_{k_{ij}}\right\}\right)$$

... then **publish MAC keys** (???) ... to enhance **repudiability**

This slide shows a little bit more detail: in addition to the new Diffie-Hellman parameter and the encrypted message, we also send along a MAC that uses a key ______________________ but which is ______________________. This means that anyone who knows the encryption key k_{ij} can ____, but it's safe for MAC keys to leak without revealing confidential information in the way that leaking k_{ij} would.

In fact, not only is it safe for MAC keys to leak, the protocol actually includes a step in which we *publish* MAC keys! Why in the world would we want to publish our MAC keys to the world?

This step enhances *repudiability*. We already know that , even without this step, ______________ ____________ can fake up a message from Alice saying $\left\{M, \mathrm{MAC}_{h(k_{ij})}(M)\right\}$. Normally, the set of people who ________________ is just Alice and Bob. However, if we publish our MAC key $h(k_{ij})$ a few messages later, it's now possible for __________________________________ to generate a MAC'ed message. This, albiet counterintuitively, *increases* Alice's privacy, since if ______________ could have generated the message, there is ________________ that Alice did beyond Bob saying so.

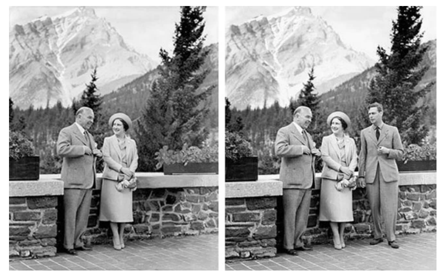
OTR benefits

Confidentiality with *forward secrecy*

Authentication with *repudiability*

Counterintuitive result:

- if anyone could've faked that photo or video or message stream...



Source: Fourandsix Technologies, Inc

- we all get (appropriately) skeptical about technical evidence's origins

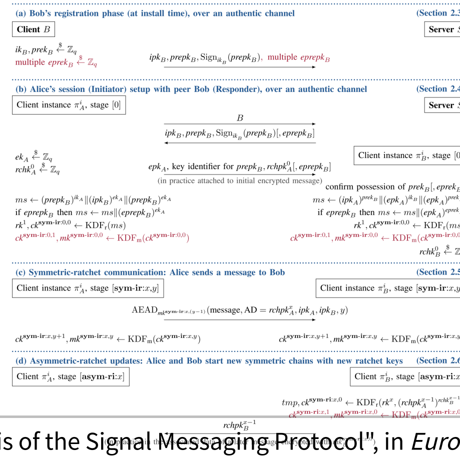
The goal of private messaging isn't to act like a confidential legal document. Instead, it's meant to act like a ________________________, in which the technology provides confidentiality and integrity properties that are ______________________ to two people talking to each other in the same room. OTR doesn't prevent your conversation partner from recording everything you say and sharing it with anyone they would like. However, it doesn't give them any technical evidence ______________ what they could take away from a private conversation (their own recollection, contemporaneous notes, etc.).

Before it became widely known just widespread photo retouching was, a photograph might've been considered iron-clad evidence that an event happened. Once we all learned just how good the pre-Photoshoppers were, however, images lost that power. Everyone knows about Stalin's zeal for erasing his enemies from photographic history, but photo tampering has been happening since the 1860s. The image on this page shows that even King George VI wasn't safe from the power of the airbrush!

Today, if you see an image of something that you don't want to believe, your first thought might well be, "it must be Photoshopped!" Soon we'll think the same thing about deepfake videos; we should already hold this level of skepticism towards chat messages.

Signal

- a wee bit more complicated!
- everywhere (e.g., WhatsApp)
- similar short-term session keys
- additional *key ratcheting*
- support **multiple devices**



Part of the Signal protocol

* Cohn-Gordon, Cremers *et al.*, "A Formal Security Analysis of the Signal Messaging Protocol", in *EuroS&P17: Proceedings of the 2017 IEEE European Symposium on Security and Privacy*, 2017, DOI: 10.1109/EuroSP.2017.27.

Almost-end-to-end messaging

Signal, iMessage, etc., support multiple devices

Requires *key distribution server*

- "dear KDS, please send me the device keys for Alice"
- need to encrypt for multiple devices
- scrutiny of this list of keys?

We now know how security protocols can be used to provide strong security and/or privacy properties in end-to-end messaging. However, what we if *want* to have more than two endpoints in communication?

A *key distribution server* can be used to keep track of all of the devices used by users and which public keys are associated with each. That way, I can send a message to ______________ __________. However, something about this should make you nervous...

... this means that you have to trust the KDS to ____ ________________

Ghost protocol

Technology embodies values, affects power dynamics, including big questions around...

Lawful interception/exceptional access

- A letter from GCHQ: "Principles for a More Informed Exceptional Access Debate"
- A response from... the Internet: "Open Letter to GCHQ on the Threats Posed by the Ghost Proposal"

Privacy-enhancing technology for you also means privacy-enhancing technology for people you might not want to have private communications. Everyone may have different thresholds of who counts as "villanous", but everyone will disapprove of at least one of the following:

- people who **criticize the government**
- people who **share misinformation**
- people who **sell illegal things**
- people who **plot acts of violence**
- people who **abuse children**

All of these people can use private messaging technology to hide their activities from law enforcement... ______________________________

Q: What do you think?

Operation Ironside

Phantom Secure (Canadian company)

AN0M*

- 27 M messages among 9,000 devices
- 800 arrests, 8 T of cocaine, 22 T of cannabis, 250 guns, $48 M
- trust issues

* Robertson, "The FBI secretly launched an encrypted messaging system for criminals", 8 Jun 2021.
Corder, Perry and Spagat, "How a Secret FBI App Kept Tabs on Crimintals in Australia, New Zealand", *Bloomberg*, 8 Jun 2021.

One alternative that law enforcement (and others) have available is going after the endpoints rather than cracking the crypto.

Phantom Secure was a company that would provide phones with private communication functionality (for over $1k per month per phone!) to large criminal organizations. The network was shut down in 2018 when the FBI arrested its CEO. This left an opening in the market for secure communications among non-techy organized crime types…

… a gap that was filled by a new system called `AN0M`, sold to criminals by someone who'd been involved in Phantom Secure. That someone was up on charges in the US, so they… offered it to the FBI!

This system, which became even more popular when BlackBerry shut down Gky Global (another Canadian company!) in 2021. Every message sent on the `AN0M` network was effectively carbon-copied to the Australian Federal Policy and the US FBI.

This led to a lot of busts, but making this arrests came at the cost of blowing the network's cover. What will criminals use next?

Just disrupting the ability of multi-national criminal organizations to communicate with confidence will have some effect on their activities. However, the crooks won't just give up: they'll try something new. When they do, law enforcement and intelligence agencies also won't just give up.

Q: How do you think free countries should balance the needs of privacy and security?

Almost-end-to-end messaging

Signal, iMessage, etc., support multiple devices

We now know how security protocols can be used to provide strong security and/or privacy properties in end-to-end messaging. However, what we if *want* to have more than two endpoints in communication?