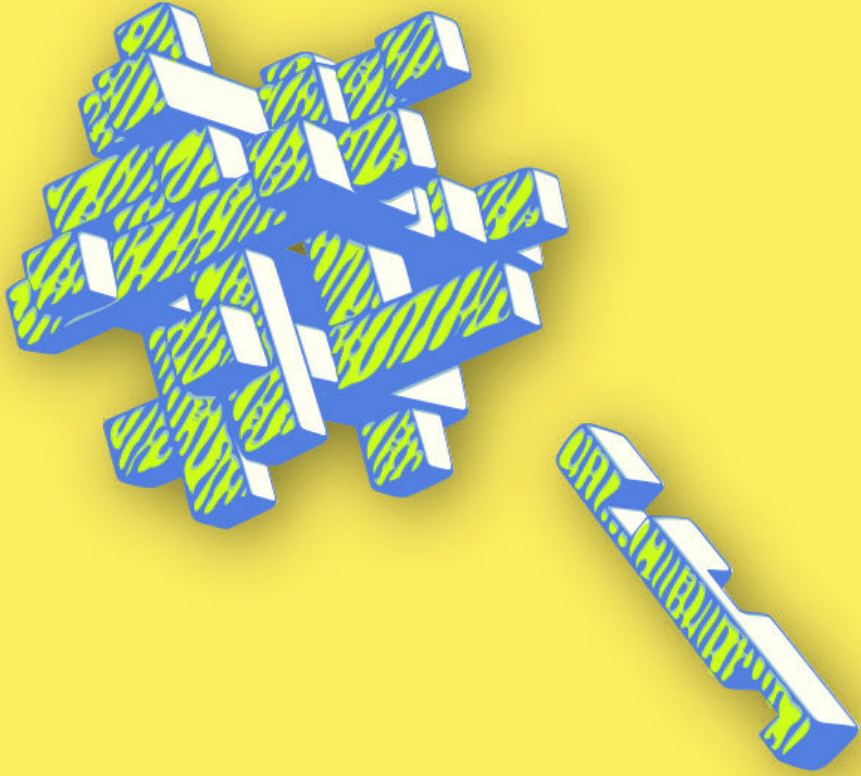




CYBERWOMEN



Encryption

Encryption

**INSTITUTE FOR
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license.

<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

Contents

1 Introduction to encryption	5
Leading the session	6
Part 1 - Have You Used Encryption Before?	6
Part 2 - Explaining Encryption	8
References	9
2 Encrypted communication	11
Leading the session	12
References	13

Introduction to encryption

- **Objective(s):** To explain to participants the concept of encryption, as well as a brief overview of the different types of encryption available to users.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
 - Basic digital security concepts and/or previous training
- **Related sessions/exercises:**
 - Privacy¹
 - Safe online campaigning²
 - Encrypted communication³
 - Storage and encryption⁴
- **Needed materials:**
 - Slides (with key points included below)
 - Laptop/Computer and Projector setup

¹<https://cyber-women.com/en/privacy/privacy/>

²<https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/>

³<https://cyber-women.com/en/encryption/encrypted-communication/>

⁴<https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/>

- Examples of encryption techniques (printed)

Leading the session

Part 1 - Have You Used Encryption Before?

1. Explain that this is an introductory session for encryption as a concept, so you will not yet be going into great depth on any of the encryption tools that participants have likely heard about before (GPG/PGP in particular).
2. Split participants up into pairs, and then start the session by demonstrating a few examples of encryption techniques. Here are a few examples that you can prepare ahead of time to share with the group:

The BLUEPRINTS Code

Each of the letters in the word Blueprints is assigned a number.

B	L	U	E	P	R	I	N	T	S
0	1	2	3	4	5	6	7	8	9

This is a specific example using a specific word, but can be broadly applied to any number and letter sequence - for instance, if you use the same system as above, the sequence of numbers 8 2 5 7 9 would spell T U R N S when "decrypted".

You could also switch the order of the numbers, so that instead of the above sequence, it now goes:

B	L	U	E	P	R	I	N	T	S
9	8	7	6	5	4	3	2	1	0

In this instance, the sequence of numbers 8 2 5 7 9 would now spell L N P U B (which isn't a word) when "decrypted"; however, you could now "decrypt" the sequence 4 3 2 0 6 as R I N S E.

Old-Fashioned Text Messaging

Use an image of an older-style phone keypad (see below) to demonstrate another kind of “encryption” that participants may be familiar with.



Old-Fashioned Text Messaging

Ask participants how they would use this keypad to spell different words – one example you could use would be to have each participant explain how they would use the keypad to spell their name. For instance, a participant named Luisa would spell her name by typing the sequence 5 5 5 8 8 4 4 4 7 7 7 2.

3. Once you’ve completed the above examples, ask participants if they have ever used other kinds of encryption – either like the above, or any other examples they can think of (e.g. a common instance of encryption used by many people every day is HTTPS).

4. Close this part of the session by following-up with another question: What are the common elements they can identify from these different examples of encryption?

Part 2 - Explaining Encryption

5. Building on the common elements of encryption identified by participants in Part 1, you should now expand on some further basics and practices for the group:

Encryption Methods: Take time to explain how encryption works, referring back to the examples from Part 1 as well as by showing a few example screenshots of what a GPG-encrypted email looks like. Highlight common implementations of encryption – in particular, spend time reviewing HTTPS, end-to-end encryption and GPG/PGP encryption.

Keys and Keypairs: Explain how encryption keypairs work, and the algorithmic relationship between public and private keys. Go back through the example implementations previously mentioned (HTTPS, end-to-end and GPG/PGP) and explain for each of these where their respective keys are stored and/or visible to the user.

Encryption Practices: Highlight some of the critical best practices associated with common implementations of encryption, such as fingerprint verification and key-signing. To demonstrate, ask participants to locate where within Signal one can verify another user's fingerprint; similarly, if participants already have GPG/PGP keys you can discuss the benefits and disadvantages of signing and distributing public keys. This is also a good time to discuss end-to-end encrypted messaging for chat apps such as Signal, Telegram and Whatsapp – remind participants that end-to-end encryption on some of these services is not always enabled by default.

Encrypted Backups: Building off the GPG/PGP example above, ask participants whether they think it is a good idea to backup their GPG pri-

vate key, and if so, how might they go about doing so?

References

- <https://www.gnupg.org/gph/en/manual/book1.html>

Encrypted communication

- **Objective(s):** To convey to participants the importance and utility of encrypting communications and providing relevant tools.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
 - Basic digital security concepts and/or previous training
 - Introduction to encryption¹
- **Related sessions/exercises:**
 - Introduction to encryption²
 - Privacy³
 - Safe online campaigning⁴
- **Needed materials:**
 - Slides (with key points included below)
 - Laptop/Computer and Projector setup

¹<https://cyber-women.com/en/encryption/introduction-to-encryption/>

²<https://cyber-women.com/en/encryption/introduction-to-encryption/>

³<https://cyber-women.com/en/privacy/privacy/>

⁴<https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/>

Leading the session

1. Start the session by sharing relevant examples of situations where encrypted communications could be useful, taking time to explain how encryption works. Demonstrate some example screenshots of a GPG-encrypted email to illustrate roughly what messages and emails look like while encrypted, and highlight common implementations of encryption – in particular, HTTPS, end-to-end encryption and GPG/PGP encryption.
2. Focus the discussion now specifically on tools that permit encrypted communications: Signal for calls and messages, meet.jitsi for video calls and Tutanota or GPG & Thunderbird for emails are good examples to share.
3. Explain the security benefits of these tools to the group, primarily how they enable users to limit others' access to their communications; then discuss situations where the security of a user's data could still be compromised, even while using encrypted communication. Ask participants – How could the contents of a GPG encrypted email be compromised by keylogging or screen-capturing malware? What if a user's private GPG key was accessed by an adversary – how could they use it to gain access to their data?
4. If time allows, participants should have the opportunity for hands-on practice with at least one of the tools mentioned above in Step 2. Although there may not be enough time to set the group up with GPG/PGP for email, you may choose to demonstrate an HTTPS protected video call using meet.jitsi, or have participants install Signal on their phones to practice sending one another encrypted messages, or to exchange encrypted phone calls.

References

- <https://ssd.eff.org/en/module/how-use-signal-android>
- <https://ssd.eff.org/en/module/how-use-signal-ios>