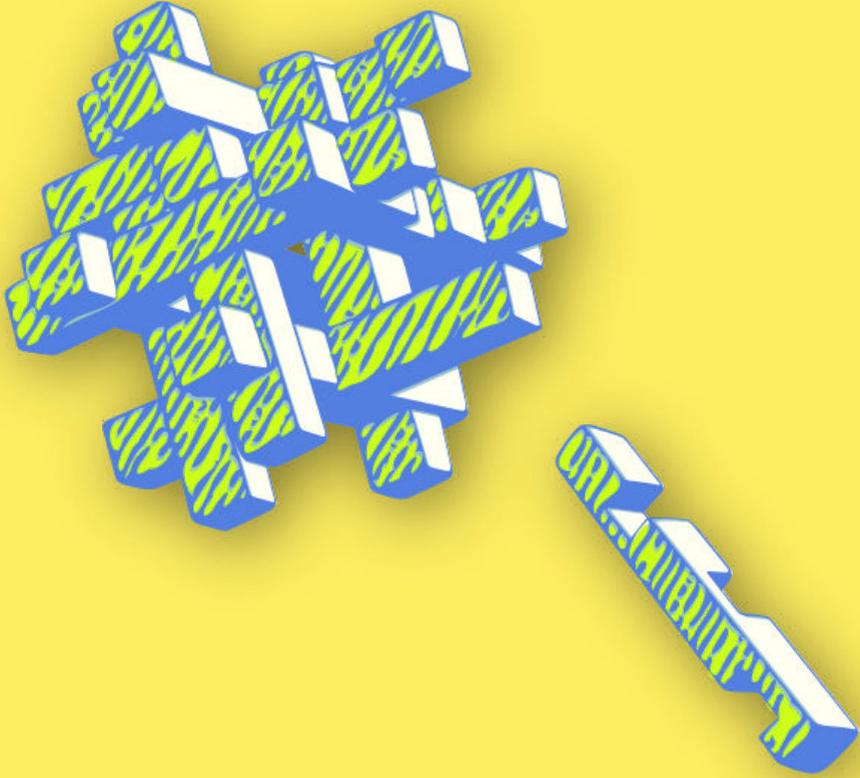




# النساء فى فضاء الإنترنت



التشفير

تعريف بمسألة التشفير

**INSTITUTE FOR  
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



نَسَبُ الْمُصَنَّفِ - الترخيص بالمثل 4.0 دولي

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

# المحتويات

٥	١ تعريف بمسألة التشفير
٦	إدارة الجلسة
٦	الجزء الأول - هل سبق لكن أن إستخدمتن التشفير؟
٨	الجزء الثاني - شرح ماهية التشفير
٩	المراجع



## باب ١

# تعريف بمسألة التشفير

- الأهداف: هذه الجلسة التعريفية ستشرح للمشاركات مفهوم التشفير، بالإضافة إلى لمحة عامة موجزة عن الأنواع المختلفة للتشفير المتوفر للمستخدمين/ات.
- الطول: 50 دقيقة
- الشكل: جلسة
- مستوى المهارة: متوسط
- المعرفة المطلوبة:
- معرفة مفاهيم الأمن الرقمي الأساسية و/أو تدريب مسبق
- جلسات/تمارين ذات صلة:
- الخصوصية<sup>١</sup>
- الحملات الآمنة على الإنترنت<sup>٢</sup>
- الاتصالات المشفرة<sup>٣</sup>
- التخزين والتشفير<sup>٤</sup>
- المواد اللازمة:

---

<https://vrr.im/819e1>

<https://vrr.im/8e6b2>

<https://vrr.im/27253>

<https://vrr.im/0ccc4>

- شرايح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- أمثلة عن تقنيات التشفير (مطبوعة)

## إدارة الجلسة

### الجزء الأول - هل سبق لكن أن إستخدمت التشفير؟

- ٠١ إشرح لمن أن هذه الجلسة جلسة ستعرفهن على التشفير كمفهوم، لذا لن نتعمق كثيراً في شرح أي من أدوات التشفير التي يحتمل أن تكون المشاركات قد سمعت عنها في السابق (لاسيما جي بي جي /GPG/بي جي بي PGP)
- ٠٢ قسمن المشاركات إلى مجموعات من شخصين ومن ثمَّ إبدأن الجلسة عبر عرض بعض الأمثلة عن تقنيات التشفير. إلیکن بعض الأمثلة التي يمكنك تحضيرها مسبقاً لمشاركتها مع المجموعة:

### شيفرة كلمة "بلورينيس" BLUEPRINTS

كل حرف من كلمة "BLUEPRINTS" يربط برقم.

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

هذا مثال محدد إستعين بكلمة محددة، ولكن يمكن تطبيقه بشكلٍ عام على أي تسلسل أرقام وأحرف - على سبيل المثال، في حال إستخدمت النظام المذكور أعلاه نفسه، تسلسل الأرقام 82579 يعني كلمة TURNS حين "يفك التشفير".

يمكنك أيضاً قلب ترتيب الأرقام بحيث يصبح التسلسل الآن كما يلي

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

في هذه الحالة، تسلسل الأرقام 82579 سيدل على تسلسل الأحرف التالي LNPUB (وهذه ليست كلمة) حين "يُفك التشفير"؛ ولكن مثلا يمكننا الآن "فكّ تشفير" التسلسل 43206 للتوصل إلى كلمة RINSE.

### الرسائل القصيرة القديمة الطراز

إستخدمن صورة لوح مفاتيح هاتف من الطراز القديم (كما يرد أدناه) لعرض نوع آخر من أنواع "التشفير" التي قد تعرفها المشاركات



### الرسائل النصية القديمة الطراز

إسألن المشاركات عن كيفية إستخدامهن اللوح المفاتيح هذا لكّابة كلمات متنوعة - أحد الأمثلة على ذلك التي يمكننا الاستعانة بها قد تكون الطلب من كل مشاركة شرح كيفية استخدامها للوح المفاتيح لكّابة اسمها. على سبيل المثال، لكّابة اسم إحدى المشاركات: لينا

Lina، نكتب تسلسل الأرقام التالي 66 2 444 555.

٣. عد أن تنتهين من عرض الأمثلة المذكورة أعلاه، سألن المشاركات إذا ما سبق لهن أن إستخدمن أي نوع من أنواع التشفير - إما نوع شبيه بالأمثلة المذكورة أعلاه وإما أي أمثلة أخرى قد تخطر في بالهن (على سبيل المثال طريقة تشفير شائعة إستخدما الكثير من الناس في حياتهم اليومية هي "إيتش تي بي إس" (HTTPS)).

٤. إختتمن هذا الجزء من الجلسة عبر طرح سؤال آخر: ما هي العناصر الشائعة التي يمكنهن تحديدها من أمثلة التشفير الأخرى هذه؟

## الجزء الثاني - شرح ماهية التشفير

٥. إستناداً إلى العناصر الشائعة من عناصر التشفير التي حددنها المشاركات في الجزء الأول، عليكن الآن التوسع وشرح المزيد من الأسس والممارسات للمجموعة:

طرق التشفير: خصصن الوقت الكافي لشرح كيفية عمل التشفير إستناداً إلى الأمثلة من الجزء الأول بالإضافة إلى عرض بعض الأمثلة عن صور ملتقطة عن شاشات لشكل البريد الإلكتروني المشفر بواسطة "جي بي جي". شددن على بعض حالات تنفيذ التشفير الشائعة - وبشكل خاص، خصصن الوقت الكافي لمراجعة تقنية "إيتش تي بي إس" والتشفير الكامل وتقنية جي بي جي/بي جي بي.

المفاتيح والمفاتيح الثنائية: إشرحن كيفية عمل مفاتيح التشفير الثنائية والعلاقة الخوارزمية بين المفاتيح العام والخاص. إستعدن الأمثلة عن التطبيقات المذكورة آنفاً (إيتش تي بي إس، التشفير الكامل وبي جي بي/بي جي بي) وإشرحن أنه لكل واحدة من هذه التطبيقات مفاتيح خاصة مخزنة و/أو ظاهرة للمستخدم.

ممارسات التشفير: ألتين الضوء على أهم الممارسات الفضلى المرتبطة بالتطبيقات الشائعة للتشفير، كتقنية التحقق من البصمة والتوقيع الرقمي على المفاتيح لعرض ذلك، أطلبن من المشاركات تحديد المكان في تطبيق سيجنال الذي يمكن للمستخدم فيه التحقق من

---

بصمة مستخدم آخر؛ وعلى نحو مماثل، في حال كانت المشاركات تمتلكن مفاتيح جي بي جي/بي جي بي، يمكنكن مناقشة فوائد ومساوئ توقيع وتوزيع المفاتيح المتاحة للعموم. والوقت مناسب أيضاً لمناقشة المراسلات المشفرة تشفيراً كاملاً في تطبيقات المحادثة كتطبيق سيجنال وواتساب وتليغرام- ذكرن المشاركات أن التشفير الكامل ليس دائماً مفعلاً بشكلٍ تلقائي على بعض هذه الخدمات.

النسخ الإحتياطية المشفرة: إستناداً إلى مثال التشفير بواسطة جي بي جي/بي جي بي المذكور أعلاه، إسألن المشاركات إذا كنّ يعتقدن أن القيام بنسخة إحتياطية لمفتاح جي بي جي الخاص بهن فكرة جيّدة، وإن كان كذلك، ما هي الخطوات التي يمكنهن إتباعها؟

## المراجع

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