AHM Homework

خوارزمية E2EE لتشفير محادثات تطبيق WhatsApp

تقديم الطلاب:

أسما نحاس asma\_128597

آية الأبيدِaya\_138463

دينا نعمة Dina\_132028

10/11/2020

**محتويات**

[**ملخص** 1](#_Toc55817862)

[**مقدمة** 2](#_Toc55817863)

[**الدراسة التحليلية** 3](#_Toc55817864)

[**أنواع المفاتيح العامة** 4](#_Toc55817865)

[**أنواع مفاتيح الجلسة** 5](#_Toc55817866)

[**إعداد جلسة المحادثات بين طرفين** 5](#_Toc55817867)

[**تشفير الرسائل** 5](#_Toc55817868)

[**خطوات الخوارزمية** 6](#_Toc55817869)

[**استقبال جلسة جديدة** 7](#_Toc55817870)

[**البروتوكولات المستخدمة** 8](#_Toc55817871)

[ Signal Protocol 8](#_Toc55817872)

[ ECDH Protocol 8](#_Toc55817873)

[**تشفير رسائل المجموعات** 10](#_Toc55817874)

[**الخلاصة** 12](#_Toc55817875)

[**المراجع:** 13](#_Toc55817876)

# **ملخص**

في عالم اليوم ، يستخدم الناس في جميع أنحاء العالم خدمات المراسلة للاتصال الآمن من أي مكان إلى أي مكان في العالم.

كما ويعد WhatsApp Messenger تطبيقًا حصريًا للمراسلة الفورية عبر الأنظمة الأساسيّة يسمح لك بتبادل النصوص والملفات وكذلك رسائل الصّوت والفيديو. مما جعله من أشهر تطبيقات المراسلة وأكثرها شيوعا لديه 1.5 مليار عميل ديناميكي في 180 دولة ولكونه تطبيقًا شائعًا ؛ كان لابد من الاهتمام بطرق خرق الخصوصيّة أمرٌ غاية في الأهمية, حيث من المهم أن تكون الرسائل المرسلة عبر الخريطة آمنة.

وبالتالي ، لإعطاء الضمان والسرية للعميل ، يتم استخدام التشفير في الغالب كالعمود الفقري للتبادلات عبر شبكة الإنترنت, حيث يستخدم WhatsApp تقنية التشفير من طرف إلى طرف ويستخدم بروتوكولات مختلفة (بروتوكول Signal ) والمفاتيح (المفتاح العام والمفتاح الخاص) جنبًا إلى جنب مع خوارزميات توليد المفاتيح مثل Curve25519 سيتم شرح هذه الخوارزمية والبروتوكولات المتعلقة بها بالتفصيل .

# **مقدمة**

ساهمت شبكة الانترنت بتغيير حياتنا اليومية بعدة طرق, وذلك على اعتبار أن هذه

الشبكة أضحت وسيلة الاتصال العالمية فقد سمحت للأفراد والمؤسسات حول العالم بتبادل رسائل البريد الالكتروني وتبعا للانتشار الواسع لتطبيقات الموبايل وظهور العديد من تطبيقات المراسلة الالكترونية كان هناك مايميز هذه التطبيقات ومن أهمها

تطبيق WhatsApp, Messenger, Telegram وغيرها .

يحظى WhatsApp بشعبية كبيرة بين خدمات المراسلة بما أنه تطبيق مجاني للهاتف المحمول تمتلكه وتديره شركة Facebook التي تساعد عملائها في البقاء على اتصال مع رفاقهم وأفراد عائلاتهم, كما يشجعهم أيضًا على إنشاء مجموعات وإرسالهم الصور والتسجيلات والوثائق والمحفوظات والتسجيلات الصوتية.

ومع تزايد عدد الأفراد الذين يستخدمون WhatsApp كوسيلة للتواصل عبر الهواتف المحمولة، ازدادت أهمية التأكد من خصوصية عملائه وأصبح الأمن أساسيًا بشكل تدريجي, حيث يتوقع عملاء التطبيق قدرًا معقولًا من الخصوصية وحماية لكل من مراسلاتهم.

لتلبية هذه الرغبة ، قدم WhatsApp في عام 2014 التشفير من طرف إلى طرف (E2EE) هذا يأخذ في الاعتبار المعلومات بين نقل الرسائل لتكون آمنة، وخالية من الاستماع خلسة وصعبة الفصل.

ولا يستطيع الغرباء أو حتى WhatsApp نفسه الوصول إليهم بهذه الطريقة، يجب فك تشفير الرسائل بواسطة المستفيد. بينما يضمن E2EE الأمان والحماية، فإنه يوفر أيضاً دوراً في زيادة القدرة على حراسة الوطن بعرقلة تبادل رسائل الإرهابيين وغيرها من المعلومات السرية التي تهدد حياة وأمن البلاد.

# **الدراسة التحليلية**

يُمكن تعريف الوسائط المتعددة على أنها المُحتوى الذي يَستخدِم أكثر من وسيط، وأصبحت الوسائط المتعددة أحد المفاهيم المهمّة نظراً لابتعاد الويب وتطبيقات الموبايل عن التصميم النصيّ واتجاهه نحو التصميم الرسومي, فالمواقع الآن تعمل على مزج النصوص، مع الصوت، والصور، ومقاطع الفيديو، لتكوين مُحتوى تفاعليّ يُقدّم تجربة حقيقيّة للوسائط المُتعددة ولكن مع الانتشار الواسع لهذه الوسائط وتبعاً للحاجة لحماية

خصوصية العملاء وبياناتهم كان لابد من وجود طريقة قادرة على منع الهجمات وانتهاك خصوصية الأفراد أثناء ارسالهم معلوماتهم الخاصة عبر الشبكة فكان لابد أن

تلجأ الشركات لخوارزميات تشفير موثوقة لجذب العملاء لاستخدام تطبيقاتها والحفاظ

على سمعتها وعملائها بآن واحد.

فكان لابد لأصحاب التطبيق الأهم في عالم التواصل الاجتماعي عبرالشبكة WhatsApp من اعتماد خوارزميات فعالة لتشفير الوسائط المتعددة التي يتناقلها العملاء على أجهزتهم .

تبعاً لتصريحات مطوري تطبيق WhatsApp إنهم لا يحتفظون بنسخة مكررة من المفاتيح الخاصة على خوادمهم إنما ينتج WhatsApp ملفات المفتاح الخاص على هاتف العميل, لكنهم يقومون بتخزين المفاتيح العامة على الخادم الخاص بهم.

وهذا لا يوجد خطر فيه، كما وتعتمد على خوارزميات التشفير End To End

التي تضمن عدم قدرة المتنصتين على الشبكة من الحصول على المعلومات المهمة وإن حصلو فهي معلومات مشفرة غير قابلة للفك إلا من قبل مستقبل هذه الرسائل حصراً فهو الوحيد الذي يملك المفتاح السري الخاص الذي يمكنه من فك تشفير الرسالة.

وفيما يلي نجد أنواع المفاتيح المستخدمة في خوارزمية التشفير:

## **أنواع المفاتيح العامة**

* مفتاح التعريف، يتم إنشاؤه أثناء تركيب التطبيق.
* مفتاح ابتدائي، ينشأ أثناء التركيب و يجدد بشكل دوري وموقع بواسطة مفتاح التعريف.
* مفاتيح الاستخدام الواحد، تنشأ حسب الحاجة.

## **أنواع مفاتيح الجلسة**

* مفتاح رئيس.
* مفتاح تسلسلي، ينشأ بالمفتاح الرئيس.
* مفاتيح الرسائل، تنشأ بالمفاتيح التسلسلية.

عند تركيب التطبيق يقوم البرنامج بإرسال المفاتيح العامة لكل من مفتاح التعريف والمفتاح الابتدائي ومجموعة من مفاتيح الاستخدام الواحد لخوادم الواتساب. يحتفظ الخادم بهذه المفاتيح على حساب المستخدم, المفاتيح الخاصة تبقى دائما مع المستخدم فقط.

## **إعداد جلسة المحادثات بين طرفين**

المراسلات في نظام التشفير الجديد كلها مشفرة وذلك يشمل رسائل الإعداد الأولي ولتحقيق ذلك يقوم المُرسل باستخدام المفاتيح العامة للمستقبل والتي يحصل عليها من خادم الواتساب. يرسل الخادم للمرسل مفاتيح المستقبل وهي مفتاح التعريف ومفتاح ابتدائي و أحد مفاتيح الاستخدام الواحد, فيقوم المرسل باستخدام مفاتيحه الخاصة و مفاتيح المستقبل العامة لإنشاء المفتاح السري (باستخدام بروتوكول ECDH) ويستخدم المفتاح السري في عملية تشفير الرسائل قبل إرسالها للمستقبل. كما يقوم المرسل بإرفاق مفاتيحه العامة مع الرسائل الأولى إلى أن يتم إنهاء إعداد الجلسة. عندما تصل الرسائل للمستقبل يقوم باستخدام مفاتيحه الخاصة والمفاتيح العامة للمرسل والتي أرسلت له مع الرسالة وينشئ منها نفس المفتاح السري الذي أنشاءه المرسل (هذه هي عبقرية بروتوكول ديفي-هيلمان) ومن ثم يقوم باستخراج المفتاح الرئيس كما فعل المرسل ويستخدمه في عملية فك تشفير الرسائل وبهذا تكون الجلسة قد أعدت بين الطرفين وكلاهما يحمل مفاتيح تشفير الرسائل.

## **تشفير الرسائل**

لكل رسالة تنشأ مفاتيح تشفير جديدة لدى الطرفين ولها هذه المميزات:

1. المفاتيح لدي الطرفين متشابهة (تبعا لبروتوكول ديفي-هيلمان)و تنشأ من مفاتيحهم العامة والخاصة.
2. مفتاح كل رسالة مستقل عن ما قبله وما بعده، فضياع الرسالة لا يوثر على سير التراسل. واكتشاف احد المفاتيح لا يمكن من فك تشفير الرسائل السابقة.
3. لا يمكن استنباط المفاتيح الأصلية من مفاتيح الرسالة.
4. المفتاح يستخدم لتشفير رسالة واحدة فقط ولا يعاد استخدامه؟

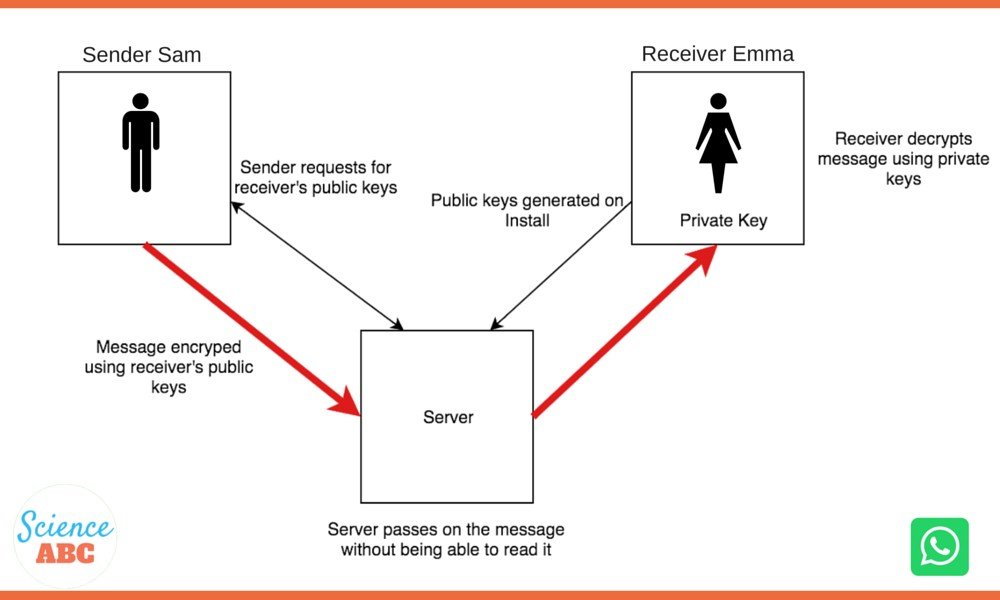
هذه المميزات تجعل عملية ربط رسالة مشفرة بمرسل معين مستحيلة، فالتحقق من صحة الرسالة ممكن لكن التحقق من هوية المرسل مستحيلة وهذه مفيدة في حال المراسلات الحساسة والتي يخشى فيها المرسل مثلا من محاكمته واتهامه بإرسال تلك الرسائل. لكن في نفس الوقت هذه الميزة تجعل عملية التحقق من هوية الطرف الآخر مستحيلة لذلك يتم استخدام مفتاح الاستخدام الواحد وكذلك خاصية التحقق من خلال تطبيق الواتساب ومطابقة رمز التحقق يدويا مع الطرف الآخر لتجاوز هذه الثغرة. ملفات الوسائط (الفيديو والصور و الصوت) والمستندات يتم تشفيرها بنفس الأسلوب. وعند استقبال ملف من شخص وتمريره لشخص آخر تتم عملية تشفير الملف بمفاتيح خاصة بالشخص اﻵخر وإرسال الملف المشفر من جديد.

### **خطوات الخوارزمية**

تصف الخطوات التالية عمل E2EE عندما يتواصل شخصان على WhatsApp:

1. عندما يفتح المستخدم WhatsApp لأول مرة ، يتم إنشاء مفتاحين مختلفين (عام وخاص) تتم عملية التشفير على الهاتف نفسه.
2. يجب أن يظل المفتاح الخاص مع المستخدم بينما يتم نقل المفتاح العام إلى جهاز الاستقبال عبر خادم WhatsApp المركزي.
3. يقوم المفتاح العام بتشفير رسالة المرسلين على الهاتف حتى قبل أن يصل إلى الخادم المركزي.
4. يستخدم الخادم فقط لإرسال الرسالة المشفرة. لا يمكن فتح الرسالة إلا من خلال المفتاح الخاص بجهاز الاستقبال. لا يوجد جزء ثالث ، بما في ذلك WhatsApp يمكنه اعتراض وقراءة الرسالة.
5. إذا حاول أحد المتسللين اختراق الرسائل وقراءتها، فسوف تفشل بسبب التشفير.

يوضح الشكل خطوات عملية التشفير من طرف إلى طرف :



## **استقبال جلسة جديدة**

للتواصل مع مستخدم WhatsApp آخر ، يحتاج عميل WhatsApp أولاً إلى إنشاء جلسة مشفرة. بمجرد إنشاء الجلسة ، لا يحتاج العملاء إلى إعادة إنشاء جلسة جديدة مع بعضهم البعض حتى يتم فقد حالة الجلسة الحالية من خلال حدث خارجي مثل إعادة تثبيت التطبيق أو تغيير الجهاز.

لتهيئة الجلسة تحدث الخطوات التالية:

1. يطلب العميل البادئ ("المرسل") مفتاح الهوية العام والمفتاح التمهيدي العام الموقّع ومفتاح مسبق عام واحد لمرة واحدة للمستلم.
2. يقوم الخادم بإرجاع قيم المفتاح العام المطلوبة. يتم استخدام المفتاح التمهيدي لمرة واحدة مرة واحدة فقط ، لذلك تتم إزالته من تخزين الخادم بعد طلبه.
3. يحفظ المرسل مفتاح هوية المستلم على أنه **Irecipient**، والمفتاح التمهيدي الموقّع ك **Srecipient**، والمفتاح التمهيدي لمرة واحدة ك **Orecipient**.
4. يقوم البادئ بإنشاء زوج مفاتيح Curve25519 سريع الزوال ، Einitiator.
5. يقوم البادئ بتحميل مفتاح الهوية الخاص به باعتباره Iinitiator.
6. يحسب المرسل مفتاح السر الرئيسي كـما يلي:

master\_secret = **ECDH(Iinitiator, Srecipient) || ECDH(Einitiator, Irecipient) || ECDH(Einitiator, Srecipient) || ECDH(Einitiator, Orecipient)**

1. يستخدم البادئ HKDF (Extract-and-Expand Key) لإنشاء مفتاح جذر ومفاتيح سلسلة من master\_secret.

## **البروتوكولات المستخدمة**

### Signal Protocol

بروتوكول الإشارة هو بروتوكول تشفير يستخدم لتوفير تشفير للنصوص والصوت والفيديو ومكالمات ومحادثات رسائل جماعية مختلفة, تمَّ تصميمه بواسطة Open Whisper Systems ، وهو أساس التشفير من طرف إلى طرف هذا هو البروتوكول الأساسي الذي يستخدم لتوفير التشفير من طرف إلى طرف.

تتضمن أهداف بروتوكول الإشارة التشفير من طرف إلى طرف بالإضافة إلى خصائص أمان متقدمة مثل الكمال, سرية التوجيه و "السرية المستقبلية".

شهد بروتوكول التشفير Signal إقبالًا كبيرًا على التشفير لملفات الاتصالات الشخصية من خلال خدمات المراسلة.

### ECDH Protocol

هو بروتوكول إدارة مفتاح يسمح للأطراف المختلفة التي لديها زوج مفاتيح بيضاوي

(أي يتم توليدها من معادلات أشكال هندسية بيضاوية الشكل) من مشاركة مفتاح سري على وسيط غير موثوق به نجد أدناه خطوات خوارزمية Diffie Helman لتبادل المفاتيح السرية:

* اختيار عددين (الأول عدد أولي q والثاني عدد صحيح أولي بالنسبة إلى q يسمى فرضا ألفا)
* بتبادل المفاتيح المشتركة بين المشترك A&b اي جهازين مختلفين (يختار A عدد عشوائي صحيح وهو أقل من q أي XA<q ) يختار b عدد عشوائي صحيح اسمه Xb ويكون xb<q أيضا)
* حساب YA& Yb
* يحسب المشترك A قيمة YA حسب المعالدلة التالية

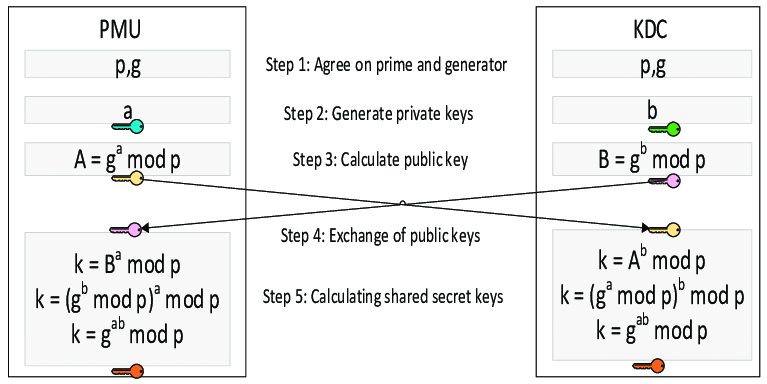
وأيضا بنفس الطريقة يحسب المشترك b قيمة Yb

* يحسب المشترك A المفتاح K حسب المعالدلة

المشترك b يحسب المفتاح K

* قيمة المفتاح k سواء تمّ حسابها من طرف المشترك الأول او الثاني سوف تعطي نفس النتيجة والقيمة

يوضح الشكل أدناه آلية تبادل المفاتيح بين المرسل والمستقبل:



### **تشفير رسائل المجموعات**

بأسلوب مشابه تقريباً لطريقة المراسلات بين طرفين يقوم المرسل عند إرسال رسالته الأولى بإنشاء جلسة للمجموعة وذلك بالتخاطب مع جميع أعضاء المجموعة كل على حدة وبتشفير مختلف عن الآخرين ويرسل لهم مفتاح موحد خاص به يسمى مفتاح المرسل. يقوم المرسل بعدها باستخدام ذلك المفتاح لإنشاء مفاتيح التشفير لكل رسالة (مفتاح تسلسلي ومفتاح الرسالة) ويستخدم تلك المفاتيح لتشفير رسائله وإرسالها للخادم والذي بدورة يقوم بتوزيع تلك الرسالة لجميع أعضاء المجموعة. جميع الأعضاء يملكون مفتاح المرسل فيقومون باستخدامه لاستخراج المفاتيح التي تتيح لهم فك تشفير تلك الرسالة والرسائل القادمة. عندما يقوم احدهم بمغادرة المجموعة يقوم بقية الأعضاء بمسح جميع مفاتيح المرسلين وإعادة إنشاء جلسات المجموعة من جديد.

##### **التخاطب مع الخادم**

بالإضافة لتشفير الرسائل بين المستخدمين فإن تطبيق الواتساب (في أجهزة الاندرويد والايفون والويندوز فون فقط) يقوم كذلك بتشفير قناة الاتصال مع الخادم وذلك يمنع من لديهم القدرة على التجسس على الشبكة من معرفة مالذي يقوم به المرسل ومع من يتحدث.

**درجة الأمان التي يوفرها التطبيق**

يوفر تطبيق الواتساب خيار يمكن تفعيلة من خلال صفحة إعدادات الأمان لتنبيه المستخدم عندما يتغير مفتاح التعريف لأي من المستخدمين المعرفين لديه. ومفتاح التعريف يتغير عند تغيير جهاز الهاتف أو إعادة تركيب التطبيق أو قيام احدهم بانتحال شخصية الطرف الآخر لذا يجب التحقق من هوية الطرف الآخر ومطابقة رمز التحقق إذا كانت سرية المحادثة مهمة.

يصعب الوثوق في تطبيق الواتساب وتشفيره لعدة أسباب منها:

1. كون التطبيق مغلق المصدر مما يصعب عملية التحقق من طريقة عملة ومطابقتها مع ما اعلن عن طريقة عمل بروتوكول التشفير.
2. كون التطبيق لا يزال يدعم التراسل غير المشفر للتوافق مع الإصدارات القديمة التي لا تدعم التشفير وأن وعملية الانتقال للتشفير تمت بشكل تلقائي من الشركة بدون موافقة المستخدم أو القدرة على اختيار نوع التراسل فهذا يعني أن الشركة قادرة على تعطيل التشفير لشخص معين دون علمه. وبما أن التطبيق يدعم التراسل بالطريقتين فالتحقق من ما يقوم به التطبيق صعب ويحتاج مراقبة مستمرة.
3. كون بروتوكول Signal مصمم في الأصل ليوفر خاصية الإنكار (repudiation وهو عكس non-repudiation) والتي تمكن المرسل من إنكار علاقته بالرسائل التي قام هو بإرسالها فإن عملية التحقق تعتمد على الثقة بخادم الواتساب بالإضافة لعملية مطابقة رمز التحقق يدويا من كلا الطرفين.

يعتبروضع الأمان في التطبيق بعد إضافة خاصية التشفير يعد افضل من السابق بمراحل عدة خصوصاً للمستخدم العادي ويعتبر من أكثر الحلول المتوفرة أمناً في تطبيقات المحادثات المشهورة حالياً.

أما من يبحث عن أمان مطلق فعليه استخدام أدوات ووسائل أخرى لا تتطلب الثقة بطرف ثالث أو استخدام عدة حلول بتقنيات مختلفة مع بعض ويعتبر تطبيق Telegram حالياً

من التطبيقات الأكثر آماناً لتبادل الرسائل والصور والفيديوهات وحفظها باستخدام الخدمات السحابية عوضاً عن حفظها في ذاكرة جهاز المستخدم.

# **الخلاصة**

الحاجة إلى خدمات الرسائل النصية والمراسلات على الهواتف المحمولة واستخدامها للتشفير من طرف إلى طرف في حماية الخصوصية تشكل قلق بعض الهيئات التشريعية حول حماية بيانات موكليها. في حين أن نسبة كبيرة من سكان الدول ستدعم وجود قيود على الوصول إلى تشفير غير قابل للاسترداد لما له من مخاطر محتملة على أمن المجتمعات. ف في الآونة الأخيرة ، تم اختراق بيانات العديد من الشركات بسبب عدم استخدام تقنيات التشفير بشكل صحيح .

لذلك كان لابد من وجود خوارزميات تشفير متينة وموثوقة قابلة لحماية البيانات ونقلها بشكل آمن فجاء تطبيق WhatsApp ليوضح أن الرسائل المرسلة من قبل المرسل يتم فك تشفيرها فقط من جانب المستلم ، ولا يمكن قراءتها بواسطة WhatsApp ولا يمكن لأي متسلل اعتراض الرسالة حيث يتم تأمين هذه الرسائل من البداية إلى نهاية التشفير كما قمنا بتوضيحه ضمن هذه المقالة بشرح خوارزمية التشفير من طرف إلى طرف حيث ينشأ العامل الهائل في توفير طبقة الأمان هذه من الاستخدام الهائل لتطبيق WhatsApp للمفاتيح المؤقتة والديناميكية.

# **المراجع:**

* CASE STUDY ON WHATSAPP END TO END ENCRYPTION- International Research Journal of Modernization in Engineering Technology and Science 2020
* pcrisk.com “WhatsApp Encryption Explained”. https://www.pcrisk.com/internet-threat-news/10240-whatsapp-encryption-explained [3] Amit Panghal “WhatsApp„s End to End Encryption”.
* Vamsi Krapa, S.Prayla Shyry, M.Rahul Sai Krishna “WhatsApp Encryption- A Research " International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019.
* https://www.ijrte.org/wpcontent/uploads/papers/v8i2S3/B10930782S319.pdf [5] “WhatsApp Encryption Overview: Technical White Paper”,WhatsApp.
* ] Whittaker, Z. (2017) US Says It Doesn‟t Need Secret Court‟s Approval to Ask for Encryption Backdoors. <https://www.zdnet.com/article/us-says-it-does-not-need-courts-to-approve-encryption-backdoors/>