الملخص

نظام التشفير يامن:
آر أس أيه المُعزز باستخدام خوارزمية رابين وترميز هافمان

اعداد : عبد الله كراكرة

اليوم، يعد نظام التفشير ال آر أس أيه مهم للغاية، فهو آلية تشفيركثيرة الإستخدام في جميع أنحاء العالم، ويستخدم في شتى المجالات ابتداء من التسوق عبر الانترنت إلى الهواتف المحمولة. ولكن هناك بعض القيود على نظام التفشير ال آر أس أيه، ومثال ذلك أن نفس الرسالة إذا شفرت أكثر من مرة بنفس المفتاح فإن النص المشفر في هذه الحالة يكون نفسه، لهذا السبب فان نظام التفشير آر أس أيه يصبح عرضة لبعض الهجمات غير المباشرة مثل العامل المشترك، النص غير المشفر المعروف، واختيار النص غير المشفر، وهجوم الوقت، وتكرار اللبنات -حسب معرفتنا لم يشر أحد مسبقا لهجموم تكرار اللبنات- وأيضا من المعروف أن نظام التفشير ال آر أس أيه أبطىء بكثير من انظمة التشفير التماثلية.

في هذه الرسالة نعرض نظام تشفير سريع وآمن من نظام التفشير ال آر أس أيه بالاعتماد على نظام تشفير رابين وترميز هافمان يسمى **بنظام التفشير يامن** لحل القيود والهجمات التي يعاني منها نظام آر أس أيه، فقد تم اضافة عنصر عشوائي على نظام التفشير ال آر أس ايه، هذا العنصر العشوائي يُشفر بواسطة نظام تشفير رابين لرفع مستوى أمان نظام التفشير ال آر أس ضد الهجمات غير المباشرة وجعله آمن دلاليا. علاوة على ذلك، **فنظام التفشير يامن** جعل من تحليل العدد إلى عوامله أكثرصعوبة، حيث يحتاج المهاجم إلى تحليل الأعداد إلى عواملها في كلا الخوارزميتين آر أس أيه و رابين لكسر نظام التفشير يامن. بجانب ذلك تم توظيف ترميزهافمان لمنع الهجمات التي قد تنتج عن تكرار اللبنات وتسريع وقت التنفيذ في نظام التفشير يامن.

فنظام تشفير يامن يحسن ثلاثة عوامل حساسة مقارنة مع آر أس أيه هي: الأمان و وقت التنفيذ وحجم النص المشفر. فنظام التشفير يامن هو آمن دلاليا، حيث يقوم بتوليد نصا مشفرا مختلفا لنفس الرسالة. بعد اختبار نظام التفشير يامن على عدة ملفات مختلفة الأحجام ابتداء من حجم واحد ميجابايت حتى حجم 10 ميجابايت أظهرت النتائج أن **نظام التفشير يامن** أكثر سرعة من ال آر أس أيه بحوالي 45% في عملية التشفير، وتقريبا 99% في عملية فك التشفير، كذلك وجدنا أن نظام التفشير آر أس آيه يزيد من حجم النص المشفر مقارنة بالنص الأصلي بـ 1% تقريبا. بينما **نظام التفشير يامن** يقلل من حجم النص المشفر مقارنة بالنص الأصلي بـ 54% تقريبا ، وهذه النسبة تعتمد على عدد الرموز المكررة داخل النص الأصلي.