La richiesta odierna era quella di decriptare un messaggio (HSNFRGH), cercando quindi di trovare il testo in chiaro. Il messaggio è stato decriptato facilmente (EPICODE) grazie all'utilizzo del cifrario di Cesare , uno dei più antichi algoritmi crittografici di cui si abbia traccia, utilizzato come dice il nome, ai tempi di Giulio Cesare. Esso consisteva in una sostituzione monoalfabetica, ovvero ad ogni singola lettera ne era assegnata un'altra che ne corrispondesse, e che, in questo caso consisteva in uno spostamento di 3 lettere in ordine alfabetico, per cui la A veniva indicata dalla D, B da E e così via.

Nel mondo odierno questo tipo di crittografia arcaica, è ormai non più utilizzata, poiché grazie al progresso tecnologico siamo giunti a 2 soluzioni: Crittografia simmetrica; Crittografia asimmetrica

La crittografia, consiste nel velare un messaggio rendendolo incomprensibile per tutti, ma leggibile soltanto a chi possiede le così dette "chiavi di criptazione/decriptazione". Al giorno d'oggi per utilizzare questa tecnica fondamentale, indispensabile in ambito della sicurezza vengono utilizzati degli algoritmi di crittografia "volgarmente" chiamati chiavi, di cui l'AES è il più utilizzato.

Entrambe le tipologie di crittografia hanno però vantaggi e svantaggi; la simmetrica, consente uno scambio sicuro e rapido, motivo per cui è utilizzata all'interno delle reti LAN, ma nel momento in cui si avrà la necessità di comunicare con un destinatario che si trova oltre la rete LAN, vi sarà un problema, poiché quando la chiave di de-/criptazione viene inviata al destinatario (la quale è la medesima per ambo le parti), questa può essere sniffata da un possibile attacco man in the middle.

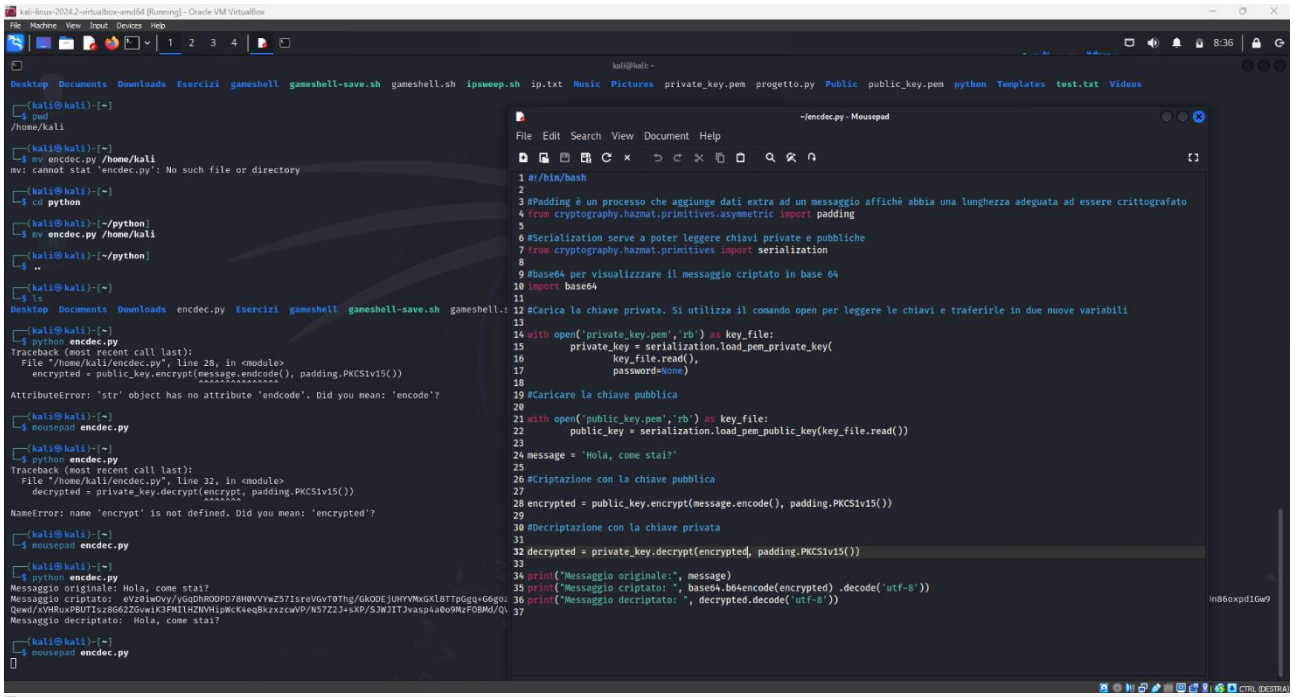
Per far fronte a ciò, la soluzione era utilizzare un altro tipo di crittografia, la crittografia asimmetrica, la quale prevede l'utilizzo di due chiavi, una privata ed una pubblica, di cui la prima servirà alla decriptazione dei file, e verrà custodita solo e solamente da una singola persona, e la seconda per criptare il messaggio. Durante il processo di scambio dati dunque, colui che sarà il destinatario, invierà al mittente la sua chiave pubblica, con la quale cripterà i dati e li spedirà al destinatario. In questo modo i dati sono sicuri al 99% poiché l'unico modo per decriptarli è utilizzando la chiave privata che possiede il destinatario. Questo processo può essere ripetuto più volte anche con chiavi differenti, e nel caso di un possibile attacco MITM anche se i dati saranno sniffati non potranno essere decriptati e quindi leggibili. Questo metodo però è comunque più lento rispetto alla crittografia simmetrica, ragion per cui oggi si utilizza un metodo che può essere considerato un ibrido tra i due.

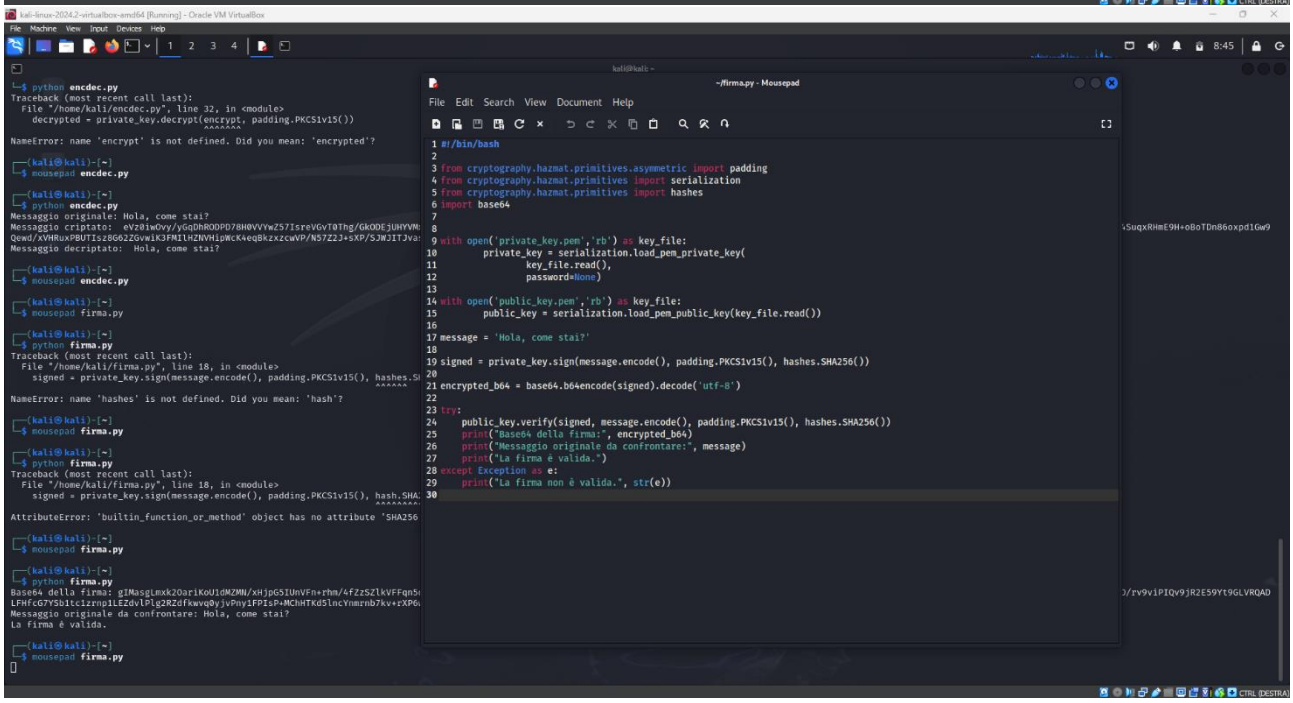
Tramite la crittografia asimmetrica verrà inviata una password (ovvero la chiave di crittografia simmetrica), che sarà spedita tramite la coppia di chiavi pubblica/privata. In questo modo è quindi possibile spedire una chiave di crittografia simmetrica, tramite il metodo asimmetrico, da un mittente ad un destinatario, senza che essa venga esposta. Sarà successivamente possibile utilizzare la crittografia simmetrica per mettere in comunicazione le due parti ottenendo una connessione sicura e con la più bassa latenza possibile, creando quello che si può chiamare un tunnel criptato, una VPN (Virtual private network) impostata sui router-gateway/gateway che fornirà una connessione molto più che affidabile e veloce.

Al fine di implementare ancor di più la sicurezza sono successivamente stati introdotti la firma digitale e il certificato digitale, i quali servono a identificare in modo assoluto e veritiero chi sia l'interlocutore con cui entriamo in contatto, e l'integrità dei file.

Per creare una firma digitale, bisognerà creare il codice hash di un file che verrà poi spedito, che successivamente verrà criptato utilizzando la chiave di decriptazione privata, e prenderà il nome di firma digitale. In seguito si dovranno fare due operazioni, la prima è la spedizione di un file in chiaro (stiamo quindi usando la crittografia asimmetrica) il cui codice hash corrisponde a quello che è stato criptato, e dopo di che verrà spedito un secondo file contenente il file digest. Il destinatario potrà quindi decriptare il digest tramite l'ausilio della chiave pubblica e avere accesso al codice hash che potrà essere confrontato per verificare l'integrità del file. Se tutto avviene correttamente saremo sicuri del nostro interlocutore.

La firma digitale però ha delle piccole debolezze, ragion per cui è stato creato il certificato digitale, il quale funziona similmente alla firma, ma qui subentra un ente di terze parti, un'autorità, C.A., che dopo aver fatto richiesta allo stato, o ad un ente che operi a livello governativo, avrà la possibilità di distribuire questi certificati. Per cui nel processo precedente, la chiave pubblica (inviata insieme alla firma digitale) risulterà modificata con più informazioni, quali il nome della C.A. con firma annessa, la data di scadenza, il nome di chi possiede la chiave ed altre informazioni. In questo modo chi riceve la chiave potrà direttamente chiedere alla C.A. competente riportata in esso, e verificare l'autenticità dell'interlocutore. In sostanza è come se spedissimo un file con la nostra firma e il timbro governativo che attesta l'identità di chi lo possiede.





In modo opzionale è stato progettato sulla macchina kali un software di criptazione e firmatura utilizzando due strumenti OpenSSL e la libreria cryptography di Python