CRITTOGRAFIA 2020/21 – Appello del 27 marzo 2021

Esercizio 1 – Chiave pubblica

Si consideri il cifrario RSA con chiave pubblica $n = 187$, $e = 9$.
Forzare il cifrario e **decifrare** il crittogramma c composto dalle due cifre centrali del proprio numero di matricola. *Riportare esplicitamente le operazioni aritmetiche eseguite.*

Esercizio 2 – Protocolli a conoscenza zero

Sia P un *prover disonesto* che afferma di essere il proprietario della chiave privata associata alla chiave pubblica $< t, n > = < 155, 187 >$.
Simulare l'esecuzione di due iterazioni del protocollo di Fiat-Shamir, esibendo tutti i valori numerici scambiati, assumendo che:

- Nella prima iterazione P utilizzi il numero casuale r composto dalle ultime due cifre del proprio numero di matricola e *correttamente* preveda di ricevere il bit 1 dal verificatore (se $r < 10$, si ponga $r = r + 10$).
- Nella seconda iterazione P utilizzi il numero casuale r composto dalle due cifre centrali del proprio numero di matricola e *correttamente* preveda di ricevere il bit 0 dal verificatore (se $r < 10$, si ponga $r = r + 10$).

Esercizio 3 – Cifrari storici

Utilizzando la cifratura di Vigenère, cifrare la frase "appello straordinario di crittografia" utilizzando come chiave il proprio cognome.

Esercizio 4 – RSA: attacchi

L'ingenuo Bob usa RSA per ricevere un crittogramma c, corrispondente al messaggio m. La sua chiave pubblica è $< n, e >$, con $n = 55$. Poiché gli sembra uno spreco usare il suo cifrario soltanto una volta, acconsente a decifrare qualunque testo cifrato gli venga inviato, ad eccezione di c, e a rimandare la risposta.
Il malvagio Eve gli invia il testo cifrato $c' = (k^e\, c) \bmod n$, dove k è la cifra meno significativa del proprio numero di matricola (se $k \leq 1$, si ponga $k = 3$).

1. Discutere se il valore di k utilizzato permette a Eve di trovare m.
2. Se necessario, modificare a piacere k in modo da poter condurre l'attacco.
3. Mostrare infine come Eve può risalire a m.