IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises VIII.

1. Consider the RSA signature scheme with $n = 85067$ and $e = 60343$. You have obtained the valid message-signature pair $(m, s) = (34152, 53384)$. Without using brute force, show that you can forge the valid signature for the message $m' = 50915$.

2. Consider a signature scheme based on the Rabin cryptosystem with secret primes p, q and public information $n = pq$. Signature of a message w are its four square roots modulo n.
   (a) Which messages can be signed?
   (b) Is the proposed signature scheme secure?
   (c) Would this signature scheme be secure if the signature is only a single square root of w?

3. Find the verification congruence in the ElGamal signature scheme variant where b is computed as

$$b = xa + rw \pmod{(p-1)}.$$

4. Consider the Lamport signature scheme with $k = 4$, one way function $f(y) = 25^y \mod 89$ and the following secret keys y_{ij}, $1 \leq i \leq 4$, $j = 0, 1$:

k	1	2	3	4
y_{k0}	33	79	63	35
y_{k1}	81	57	45	10

   (a) Compute the public keys z_{ij}.
   (b) Sign the message 1001 and then verify the signature.

5. A shift cipher key is exchanged using the Diffie-Hellman key distribution with $q = 5$ and $p = 47$. The actual numbers exchanged were $X = 38$ and $Y = 3$. Find the key and decipher the message:

```
EQPITCVWNCVKQPU
```

6. Consider the Ong-Schnorr-Shamir subliminal channel with public key $(h, n) = (36606, 47371)$. Alice wanted to be sure her secret message gets to Bob so she sent the same secret message w twice using the signed messages $(11587, 46420, 41083)$ and $(3561, 41492, 25348)$. Perform the following tasks:
   (a) Verify the signature for both messages.
   (b) Without using brute force, find the secret message w and the secret key k.

7. Consider the Lamport signature scheme with messages of length $k \in \mathbb{N}$.
   (a) If the scheme is used $t \geq 2$ times to sign completely random messages, what is the probability that Eve, who intercepts the signatures, will be able to forge a signature of any possible message of length k?
   (b) If $k = 5$, what is the least number of times the scheme needs to be used so that Eve, who intercepts the signatures, will be able to forge a signature of any possible message of length 5 with at least 85% probability?