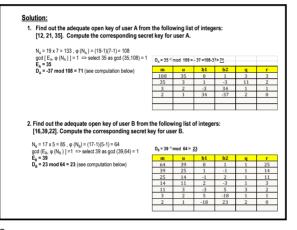
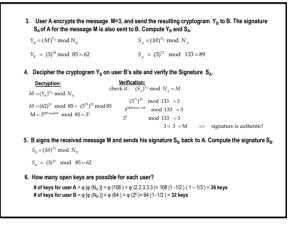


- P1: A RSA cryptosystem with two users A and B having the secret prime number (10 P) pairs for A: 19 and 7 and for B: 17 and 5 is used
- 1. Find out the adequate open key of user A from the following list of integers: [12, 21, 35]. Compute the corresponding secret key for user A.
- 2. Find out the adequate open key of user B from the following list of integers: [16,39,22]. Compute the corresponding secret key for user B..
- 3. User A encrypts the message M=3, and send the resulting cryptogram  $Y_B$  to B. The signature  $S_A$  of A for the message M is also sent to B. Compute  $Y_B$  and  $S_A$ .
- 4. Decipher the cryptogram  $Y_{B}$  on user B's site and verify the Signature  $\,S_{A}^{}.\,$
- 5. B signs the received message M and sends his signature  $S_{\rm B}$  back to A. Compute the signature  $S_{\rm B}.$
- 6. How many open keys are possible for each user?

2



3



4

Solution:
K= 56 Bits, H(x)=90 Bits, r = 0.1
1. Unicity distance $n_u = K/r = 56/0.1 = 560$ Bits
As r=[N-H(x)]/N ⇒> N.r=N-H(x) => Block size N=H(x)/(1-r) ⇒ N=90/0.9=100 Bits
2. New unicity distance $n'_u = 2 \times 560 = 1120$ Bits
$n'_{u}$ = K/r' => r' = K/n'_{u} => the new resundancy r'= 56/1120 = 0.05
The new block size N' = H(x) / (1-r') = 90 / (1 - 0.05) = 94.74 $\approx$ 95 Bits
3. $n'_u = (L + N) / N \cdot n'_u = (10 + 95) 95 \times 1120$ $n'_u \approx 1238 Bits$
4. The observer can not theoretically break the cipher as the number of the observed cryptogram bits (1000 bits) are less than the unioty disclance (1238 bits) of the cipher.

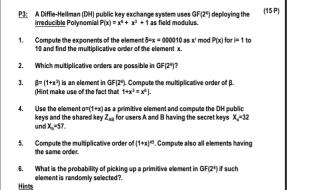
<u>P2:</u> A block cipher having a key size of 56 bits is encrypting a clear text with the entropy of 90 bits. The clear text redundancy is r=0.1. (8 P)

- 1. Compute the cipher's unicity distance n<sub>u</sub> and its block length N.
- 2. The unicity distance was doubled by data compression. Compute the new resulting data block length.
- After compression as in (2), the "unicity distance" was enhanced by appending 10 random bits to the clear text block. Compute the new resulting unicity distance.
- 4. After all the above cipher changes an observer was able to watch 1000 cipher text bits. Would the observer with unlimited resources theoretically be able to break the cipher in that case ? Give a reasoning for your answer.

Page 2/5

6

5



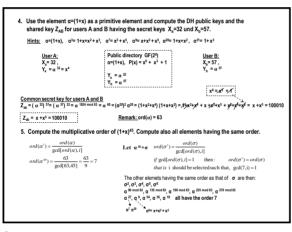
 $\overline{\alpha^{=}(1+x)}$ ,  $\alpha^{3}=1+x+x^{2}+x^{3}$ ,  $\alpha^{7}=x^{2}+x^{5}$ ,  $\alpha^{9}=x+x^{2}+x^{5}$ ,  $\alpha^{20}=1+x+x^{2}$ ,  $\alpha^{21}=1+x^{3}$ 

7

```
Solution:
1. Compute the exponents of the element \delta=x = 000010 as x<sup>i</sup> mod P(x) for i= 1 to 10 and find the multiplicative order of the element x.
                        P(x) = x^6 + x^3 + 1 = 0 \implies x^6 = x^3 + 1
                     \begin{split} \mu(x) &= x_1 + x_2 + 1 = 0 \quad \Rightarrow \quad x^* = x^* + 1 \\ &x^2 = x^2 + 1 \\ &x^2 = x^2 + 1 \\ &x^2 = x^2 + x \\ &x^2 = x^2 + x^2 + 1 + x^2 = 1 \\ &\Rightarrow multiplicative order of x is 9 \\ &y^2 = x^* = x^2 + 1 + x^2 = 1 \\ &\Rightarrow multiplicative order of x is 9 \\ &y^2 = x^* = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 = 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 + x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 = x^2 + 1 + x^2 + 1 \\ &= x^2 + x^2 + 1 + x^2 + 1 \\ &= x^2 + x^2 + 1 + x^2 + 1 \\ &= x^2 + x^2 + 1 + x^2 + 1 \\ &= x^2 + x^2 + 1 + x^2 + 1 \\ &= x^2 + x^2 + 1 + x^2 + 1 \\ &= x^2 + x^2 + 1 + x^2 + 1 \\ &= x^2 + x^2 + 1 + x^2 + 1 \\ &= x^2 + 
                          ×10 = ×
       2. Which multiplicative orders are possible in GF(26)?
                                 Possible orders are the divisors of 2<sup>6</sup> -1 = 63
Divisors of 63 are: 1, 3, 7, 9, 21, 63

    β= (1+x<sup>3</sup>) is an element in GF(2<sup>6</sup>). Compute the multiplicative order of β.
(Hint make use of the fact that 1+x<sup>3</sup> = x<sup>6</sup>).
```

8



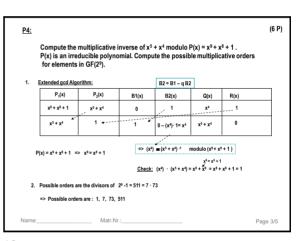
9

1.

2.

3.

4.



10

12

