Information Security CW2 nkatz01_20/01/2020

1 RSA encoding

1.

n = 143

M = 120 (120 is co-prime with n)

f = (p -1) (q-1) = 120

e = 11

d = 131

e*d = 1441

1441 mod 120 = 1

Explanation: I saw here https://mathcs.clarku.edu/~djoyce/ma126/11times13.html that one can use 7 for e and 103 for d so I tried seeing what I would need to make d as if I wanted to use 11, which is the next one up in the row of co-primes to 120, for e. See link: https://tio.run/##y0rNyan8/z/98ISHO5v@H25/1LTG/f//aEMjg1g

I achieved it by composing a number that is both, divisible by 120 with a remainder of 1, and divisible exactly by 11.

The process was roughly:

First composing a number that are multiples of 11 and 120:

11*120 = 1320

And then adding a number z to 1320, such that z is a multiple of 11 but is only short (or in excess) of one digit from being a multiple of 120, hence **121** (Although I could have used 121 itself for e*d = 11*11, I didn't feel comfortable having e and d the same number). So:

1320 + 121 = 1441

And then dividing 1441 by 11, gave me d: 1441 / 11 = 131

2.

120^11 = 74300837068800000000000

74300837068800000000000 **Mod** 143 = **87**

(87 ^ 131 = 1.19404884550027513383300108330694e+254

1.19404884550027513383300108330694e+254 **Mod** 143 = **120)**

So, in the encryption phase, 120 is replaced by 87.

Or, in general, by repeated squaring with modular exponentiation:

Encryption

Multiply together, from R – L, only where binary position has 1	$* x^8$	$* x^4$	$* x^2$	$* x^1$
Decimal exp 11 in binary =	1	0	1	1

x = 120

120 * 120 ^ 2 = 1728000

1728000 Mod 143 = 131

131 * 120 ^ 8 = 5632760217600000000

5632760217600000000 Mod 143 = **87**

Decryption

Method

X = 87	Begin with x	Square	Square	Square	Square	Square	Square & mul by x	Square & mul by x
Dec Exp 131 =	1	0	0	0	0	0	1	1

Process

Compute	**Take the mod**	**Exponent in Bin – L - R**
87		1
sqr(87) = 7569	7569 Mod 143 = 133	0
sqr(133) = 17689	17689 Mod 143 = 100	0
sqr(100) = 10000	10000 mod 143 = 133	0
sqr(133) = 17689	17689 Mod 143 = 100	0
sqr(100) = 10000	10000 mod 143 = 133	0
sqr(133) * 87 = 1538943	1538943 Mod 143 = 120	1
sqr(120) * 87 = 1252800	1252800 Mod 143 = **120**	1

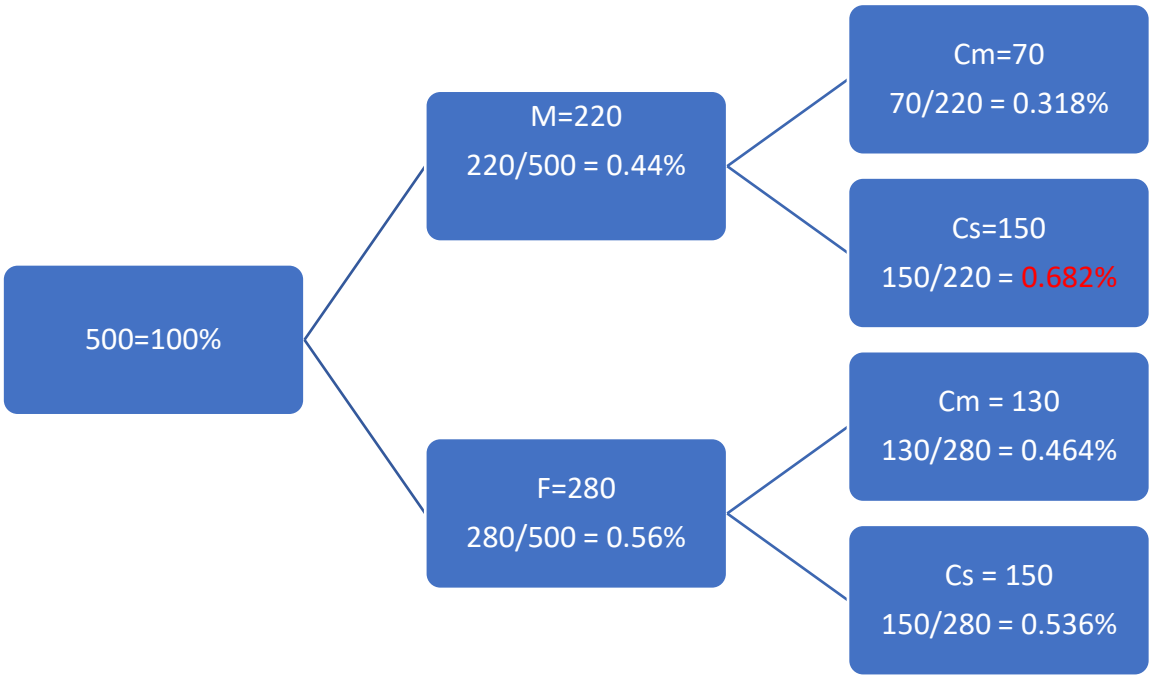
2 Conditional Probabilities

1.

Cm: 130 females and 70 males

2.

Answer: 0.68%



3.

M = male, F = female, Cs = Computer Science, Cm = Computer Management.

P(A) = P(Cs) = 300/500 = 0.6

P(B) = P(M) = 220/500 = 0.44

P(B|A) = P(M|Cs) = 150/300 = 0.5

P(A|B) = P(A)*P(B|A)/P(B) = 0.6 * 0.5 /0.44 = **0.682**

3 Quality of spam filtering

1. 1/98%, because 1% is indeed spam.
2. 2/98%, because the spam filter maybe 100% ineffective
3. 50%, eg. If the filter is a good one: $\frac{1}{2} = 50\%$
4. 100%, if filter is 100% ineffective: $\frac{2}{2} = 100\%$