FUNDAMENTAL CONCEPTS OF CRYPTOGRAPHY

ASSIGNMENT TWO

NICHOLAS KLVANA-HOOPER (19782944) – 15/05/2020

Question 1

2) GCD (2543, 1672) is 1 with s = 215 and t = -327

3) Prove this statement: $\gcd(a, b) = \gcd\big(b, a.mod(b)\big)\, for\ (a > b)$

Say equation 1: $c = a.mod(b)$ then, $\gcd(a, b) = \gcd\ (b, c)$

Say equation 2: $a = by + c$ then c could be established as 3: $c = a - by$

This would mean if $d|b,\ d|c$ then this would mean $d|a$
And if $d|a,\ d|b$ then this would mean $d|c$

So any common divisor of *a* and *b* would be a common divisor of $a - by$, using equation 3 we could say that a $\gcd(a, b)\ |$ c and as such we also say $\gcd(a, b)$ | b which together we say therefore $\gcd(a, b)$ | $\gcd(\mathrm{b}, \mathrm{c})$ and by expansion $\gcd(a, b)$ | gcd $(b, a.mod(b))$

Next, since any common divisor of *b* and *c* would be a common divisor of $by + c$, using equation 2 we could then say that $\gcd(b, c)$ | a and as such could also say $\gcd(b, c)$ | b which together is $\gcd(b, c)$ | gcd (a, b) and by expansion $\gcd\big(b, a.mod(b)\big)$ | gcd (a, b)

Since both $\gcd\big(b, a.mod(b)\big)$ | $\gcd(a, b)$ and $\gcd(a, b)$ | $\gcd\big(b, a.mod(b)\big)$ we can follow that $\gcd(a, b) = \gcd\big(b, a.mod(b)\big)\, for\ (a > b)$

Question 2

Original Text:

For example as pointed out by researcher. For each set of fuzzy terms, $A \subseteq M$, $\prod_{m\in

A}m$ represents a conjunction of the fuzzy terms in A. For

instance,

let $A=\{m_{1,2},m_{2,1},m_{4,2}\}\subseteq M$, a new

fuzzy concept ``$m_{1,2}$ and $m_{2,1}$ and $m_{4,2}$" with the linguist

interpretation ``\emph{short sepal and wide sepal and narrow petal}"

can be represented as $\prodfh

NOTE: This is shorter as I made it so the ciphertext for this would fit on one page

Cecrypted text with p=10007, q=52121, e=25537

For example as pointed out by researcher. For each set of fuzzy terms, $A \subseteq M$, $\prod_{m\in

A}m$ represents a conjunction of the fuzzy terms in A. For

instance,

let $A=\{m_{1,2},m_{2,1},m_{4,2}\}\subseteq M$, a new

fuzzy concept ``$m_{1,2}$ and $m_{2,1}$ and $m_{4,2}$" with the linguist

interpretation ``\emph{short sepal and wide sepal and narrow petal}"

can be represented as $\prodfh

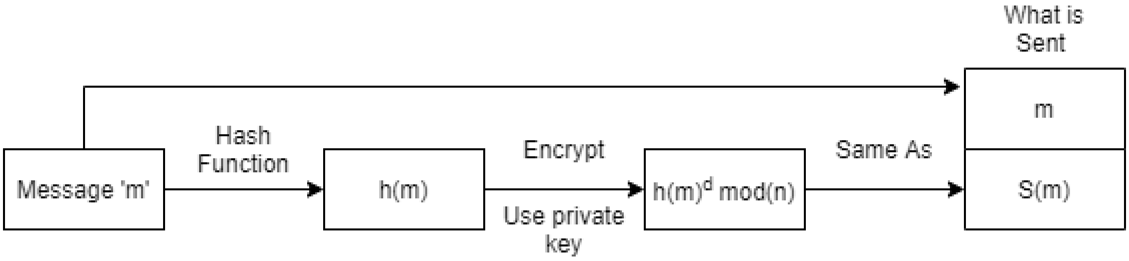
Cipher text with p=10007, q=52121, e=25537

```
396718713,243165040,124159753,501745882,45510371,123270073,394376890,449406297,374093
100,81958626,45510371,501745882,394376890,412917588,501745882,374093100,243165040,352
919765,40263658,119753139,45510371,129395635,501745882,243165040,195782056,119753139,
501745882,326063704,482857730,501745882,124159753,45510371,412917588,45510371,3943768
90,124159753,434587804,267577422,45510371,124159753,25230260,501745882,396718713,2431
65040,124159753,501745882,45510371,394376890,434587804,267577422,501745882,412917588,
45510371,119753139,501745882,243165040,272681844,501745882,272681844,195782056,264862
402,264862402,482857730,501745882,119753139,45510371,124159753,449406297,412917588,28
0895377,501745882,417516626,297787375,501745882,505546589,412917588,195782056,3260637
04,412917588,45510371,119753139,45510371,198076322,501745882,52497663,417516626,28089
5377,501745882,417516626,505546589,374093100,124159753,243165040,129395635,255302601,
206155709,449406297,505546589,352919765,40263658,371896273,297787375,453064844,449406
297,417516626,501745882,124159753,45510371,374093100,124159753,45510371,412917588,455
10371,40263658,119753139,412917588,501745882,394376890,501745882,434587804,243165040,
40263658,476540999,195782056,40263658,434587804,119753139,352919765,243165040,4026365
8,501745882,243165040,272681844,501745882,119753139,267577422,45510371,501745882,2726
81844,195782056,264862402,264862402,482857730,501745882,119753139,45510371,124159753,
449406297,412917588,501745882,352919765,40263658,501745882,417516626,297787375,417516
626,25230260,501745882,396718713,243165040,124159753,371896273,352919765,40263658,412
917588,119753139,394376890,40263658,434587804,45510371,280895377,371896273,501745882,
81958626,45510371,119753139,501745882,417516626,297787375,373047187,505546589,2061557
09,449406297,255302601,206155709,335271736,280895377,332565621,453064844,280895377,44
9406297,255302601,206155709,332565621,280895377,335271736,453064844,280895377,4494062
97,255302601,206155709,338453863,280895377,332565621,453064844,505546589,453064844,50
5546589,412917588,195782056,326063704,412917588,45510371,119753139,45510371,198076322
,501745882,52497663,417516626,280895377,501745882,394376890,501745882,40263658,455103
71,458320916,371896273,272681844,195782056,264862402,264862402,482857730,501745882,43
4587804,243165040,40263658,434587804,45510371,374093100,119753139,501745882,424060151
,424060151,417516626,449406297,255302601,206155709,335271736,280895377,332565621,4530
64844,417516626,501745882,394376890,40263658,129395635,501745882,417516626,449406297,
255302601,206155709,332565621,280895377,335271736,453064844,417516626,501745882,39437
6890,40263658,129395635,501745882,417516626,449406297,255302601,206155709,338453863,2
80895377,332565621,453064844,417516626,303436972,501745882,458320916,352919765,119753
139,267577422,501745882,119753139,267577422,45510371,501745882,81958626,352919765,402
63658,289282609,195782056,352919765,412917588,119753139,371896273,352919765,40263658,
119753139,45510371,124159753,374093100,124159753,45510371,119753139,394376890,1197531
39,352919765,243165040,40263658,501745882,424060151,424060151,505546589,45510371,4494
06297,374093100,267577422,206155709,412917588,267577422,243165040,124159753,119753139
,501745882,412917588,45510371,374093100,394376890,81958626,501745882,394376890,402636
58,129395635,501745882,458320916,352919765,129395635,45510371,501745882,412917588,455
10371,374093100,394376890,81958626,501745882,394376890,40263658,129395635,501745882,4
0263658,394376890,124159753,124159753,243165040,458320916,501745882,374093100,4551037
1,119753139,394376890,81958626,453064844,303436972,371896273,434587804,394376890,4026
3658,501745882,326063704,45510371,501745882,124159753,45510371,374093100,124159753,45
510371,412917588,45510371,40263658,119753139,45510371,129395635,501745882,394376890,4
12917588,501745882,417516626,505546589,374093100,124159753,243165040,129395635
```

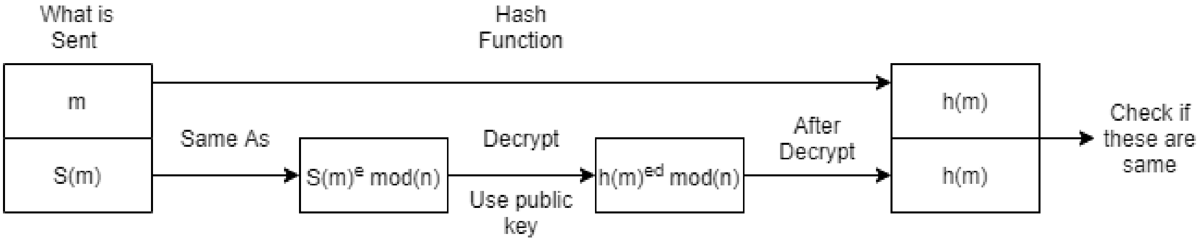
Question 3

The RSA signature structure depends on having a keyholder who can encrypt a message with a private key while everyone who is sent decrypts this message with their public key

Sender's Signature:



Sender Authentication:



As part of the RSA signature scheme, the sender will have a message that they will hash to make it a certain length. Then, this hashed message is encrypted using the sender's private key which makes up the sender's signature. The sender will send this signature and the message to the recipient.

The recipient receives the signature which it then decrypts using its public key, the two keys will multiply and mod by n to produce just the hashed version of m. The recipient then, also takes the message sent and hashes that as well. It will compare both hashed messages, if these are the same then the authentication of the sender is achieved.

The hash function is created to have very low collision so that there are rarely collisions. But in this case Bob has two messages (*m* and *m*') that hash to the same value but aren't equal. In this way Bob already has Alice's encrypted version of h(m) which is her certificate. Bob could send this encrypted version of Alice's original h(m) along with m'. The recipient of bob's message would decrypt Alice's encrypted h(m) and end up with h(m) and would then hash the *m'* to get h(*m'*) . We know that h(m) and h(*m'*) are the same so therefore this recipient would think that Bob is Alice. Thus successfully forging her signature.

Question 5

Based on the lecture slides, the probability of at least one match is:

$$1-\left(1-\frac{1}{n}\right)^{k}$$

In this question there is a group of 24 people that can be chosen, allowing for this many combinations of two people.

$$\frac{24!}{22!*2!}=\frac{24*23}{2}=276$$

So there are a total of 276 combination of 2 people in a group of 24 people

With k = 276, and n=365 we get this:

$$1-\left(1-\frac{1}{365}\right)^{276}$$

This results in a probability of 0.531