```
#he variables e and n represent the public key components: e is the public exponent, and n is the modulus.
#ct is cipher text
# b"the string" ---->represent byte object
#int.from_bytes() is a method in Python that converts a sequence of bytes into an integer. It takes two parameters: the bytes to convert and the byte order ('big' or 'little').
#"big" is used as the byte order parameter, which means that the most significant byte is at the beginning of the byte array.
# f = pt.to_bytes(pt.bit_length(),"big")---> to convert back to byte array
#ϕ = (p-1)(q-1),n = p*q
# gympy2 for arithmetic precision.
#msg = pow(signature,e,n) --> decrypts


# e = 65537 #n=1357710300952485642173335487080859767066354702016933829773598844057850532336246692097984881143326212510718962230463038903561779272603619225672552782635164311103480359123
# string = b'CottonCandyCyan'
# t = int.from_bytes(string,"big")
# s = pow(t,e,n)
# print(s)


# ct = 65730873122241583977501942857521551655862419814142537467794605641487141508168112705849405463650251324036527189894154256188004834922930955553552265141530965811260529590272915364
# d = 89251284341640489096918922591701257646451917214324437853236147012137012639315313697720086398595718844693820299212053952353479400606835246986852876111439523655259986719375825328211
# n = 10000446951441430558975509368938836249573464350273859948003996181799321930830582516340368101051064499785773467172953290947837202047478477657338650951812982110804689066962233756681
# pt = pow(ct,d,n)
# print(pt)
# f = pt.to_bytes(pt.bit_length(),"big")
# print(f)

# p = 285880804885505715088365434821249117591
# q = 223548505081667812376946559606986057893
# phi = (p-1)*(q-1)
# print(phi)

# e = 65537
# phi = 60405307365679473695011595103128719128176824853854670380659392210778713718677526218707654799173300354387162857343160755894610700871253076565877380345494 24
# d = (pow(e,-1,phi))
# print(d)

# ct = 5119667904388996554913075691965298077574451428525647832421139040755532148564677239610936209568188199266675953600861923623367821617006732308102397661359638
# n = 6910782171213996658397253121710630123795235324197483219005527369298065059694620267925472189305202037262152652525687783466320955431741311010423968405213211
# e = 65537
# p = 778752131537381834571698668351336101557723140728231330212504334143010220766 77
# q = 887417432498194548032561287244226647797723075936664731140323701337485686693 43
# phi = (p-1)*(q-1)
# d = pow(e,-1,phi)
# print(d)
# pt = pow(ct,d,n)
# ct = pt.to_bytes(pt.bit_length(),"big")
# print(ct)

# import gmpy2
# n = 1170747127492433141041202065232088282397393563708132712318124208426597574275534552825593712158750816818117537381350755744975049991884205189251550462350357516394043890718355537321
# e = 3
# ct = 8289500602102531521219476681895977818007154002572409923541320981907276652240946278095987536043114545551856046147274554910030658807410677155239997984613571622794254118050939919343
# dec = gmpy2.iroot(ct,e)[0]
# dec_int = int(dec)
# decoded_msg = dec_int.to_bytes(dec_int.bit_length(),"big")
# print(decoded_msg)

#FIND THE MESSAGE FROM THE SIGNATURE =>

# p = 14142576175088243436611365603746552806444693459074754759191307124755807147852306777542433937990254914068238812124659214675533210970490138667155888686046871028957355803052736187
# q = 15700605155155474944794846115416606928074123353990903887712229662815525047202777873958621029128492467226439817899770483875319707358855377189482808032161924249558621406803643285
# e = 65537
# signature = 21127256972405957923387011048400011431059653140091568867584307537291932809179496459498207512119297630904379849803010372724832459871218654257328645476196081067340401201618
# n = p*q
# msg = pow(signature,e,n)
# print(msg)
# ans = msg.to_bytes(msg.bit_length(),"big")
# print(ans)
```