▓WPA2 where CTR mode where CBC mode?

▓WPA2-PSK what PSK stand for?

▓RC4

▓How random number generated by programming languages and why are they not crypotographically secure? They generated by linear congruential generator

▓how does your laptop the master key?

▓the consequence of your being able to predict the next number? Get the session key

▓most popular ?X7.9

▓what is the fastest way to find k and q for miller Rablin algorithm p-1 = 2^k \* q? shit the bit pattern for p-1 to the right until the least significant bit is 1

▓the naïve brute-force implementation for testing a vary large p? exponential algorithm

▓chinese algoritm?factorize the modulus into a small set of probes

▓chinese CRT ans:15

▓why do we need “equal to n” in the definition of totient to n? no number is coprime to itself and totient of 1 is 1

▓F theorm for primarity checking, E theorm for RSA

▓What do we get by placing that condition (n is product of 2 primes) on the modulus n? so M doesn’t need to be coprime to n

▓Why breaking RSA means figuring out the prime factors p and q of the modulus n? so totient of n is (p-1)\*(q-1)…

▓1024-bit RSA for encrypting message, if m is short (small) and e=3, why can’t attacker decrypt the message by the cube-root of c? the padding rule is unknow so attacker cannot unppading m from 1024-bit block

▓Why writing interger into bit representation (2 exponential form) can speed up the computation of A^B mod p? summation?

▓definition of certificate? Public, hash, signed

▓message exchanged subsequently between you laptop and amazon.com? laptop order book-> amazon send laptop a certificate (amazon also send all the keys for itermidiare CA)-> use public key of root CA reloaded in laptop to decrypt (verify) the certificate

▓in ecommerce transaction only Amazon send certificate to laptop and laptop authenticating Amazon. Amazon don’t authenticate laptop

▓magic of DH algorithm? Two parties configure the session key without transmission

▓how DH create session key?

▓ECDH how to create public key, private key, session key?

▓what is the point of adding a single bit of value 1 at the end of the message? Soit won’t crash due to see the end of file

▓why do we include the length of the message in what gets hashed? Makes it more difficult to change the message

▓why can a hash function not be used for encryption? One-way property

▓strong collision resistance property of a hash function?

▓create a new password, only hashcode for password is stored, text you entered is immediately discarded.

▓birthday attack? The probability that a pair of people have the same birthday

▓relationship between hash in hashing function and hash in hash table?