20865679
jeadie
Jack Eadie
Written Questions

Question 1

a) Xor of the original two plaintexts can be found in the file named, xor.

b) Given an individual plaintext is irrecoverable various techniques can be used to piece together at least one of the plaintexts (which than, simply xored will produce the other). Firstly, due to the character limitations, it is more simply to guess which characters are spaces. Only spaces numbers and special characters have the sixth bit set. Thus, any xor text with this bit set has one of the corresponding plaintexts as either a space, number or plaintext (this obviously ignores characters where both plaintexts have these characters, although this type of collision is less occuring). It is further assumed that any occurence of this sixth bit is a space, rather than a number or special character. This, then, provides divisioning of possible words for a plaintext as well as the other text's character (xoring a space with the xored text produces a plaintext character). Smaller words can then be guessed, or lower syllables analysed (like bigrams, trigrams, etc).

A technique also used to guess potential words was a standard crib search using 5000 common english words. This pairing (of quadratic complexity) checks all possible pairings of words and checks if their xor is within the xored plaintext. The result of this gives a mapping of potential word pairings and their location in the xor text.

Question 2

a) Verification key is correct, so Alice's browser will think it has come from a valid CA. Assumedly Mallory will set the hostname accordingly (she has the signing key) and thus Alice will establish the TLS connection to the phishing site.

b) No. Because the actual CA certificate is being used Alice's browser will check the certificate and confirm that its hostname matches that of the phishing website. It of course doesn't and the TLS connection will not proceed.

c) Yeah, that'll work. This time when Alice's browser goes to check the hostname, they will match yet the underlying IP address will be that of Mallory's phishing site (that if contacted outside the DNS poisoning, would have a different hostname).

d) Yes, Because Mallory will know the key pair (they are the same across devices), So she will be able to create a CA certificate that, when received, will be accepted by Alice.

e) In this case Mallory will not know the key pair to create a certificate that appears to be from the Root CA.

Question 3

a) Commands

a = SELECT SUM(Expected Salary) FROM Alumni WHERE Gender == "F" or Name == "Cori"

b = SELECT SUM(Expected Salary) FROM Alumni WHERE Gender != "F" or Name == "Cori"

c =SELECT SUM(Expected Salary) FROM Alumni

Result: a + b -c

Must assume distribution of entries for Gender is close to equal so that `a = SELECT SUM(Expected Salary) FROM Alumni WHERE Gender == "F"` is between 2N/8 and N-2N/8

b) Firstly, note we can find gender field of rachel via the difference in the following two queries:

b) `SELECT COUNT(*) FROM Alumni WHERE Gender == "M"`

a) `SELECT COUNT(*) FROM Alumni WHERE Gender == "M" or name="Rachel"`

Suppose Rachel's record is "M". Then we can perform binary search based on the following queries:

c) `SELECT COUNT(*) FROM Alumni WHERE Gender == "M" or name="Rachel" or salary > X`)

d) `SELECT COUNT(*) FROM Alumni WHERE Gender == "M" or salary > X`)

Like the Gender field query if c-d is zero, then we know Rachel's salary is > X. Because we know the domain of possible salaries (between 0 and $200,000), then we are able to perform binary search to find her salary. Again, relies on the distribution of genders like part a.

If a-b is zero, then we know Rachel has field Gender == "M" (and obviously Gender == "F" otherwise).

Question 4

a) Institute of scrap recycling industries (ISRI) petitioned for two expansions. Firstly, they want the previous limitation, enacted in 2010, that unlocking of wireless devices be restricted to used devices. Initially this proposal was adopted because of concern that they would take advantage of discounted phone pricing, unlocking the carrier and resaling for a profit. This limitation, it is argued, is outside the scope of copyright protection.

Secondly, they wanted the list of device categories allowed for unlocking to be removed so that any device with wireless capacity is exempt from unlocking restrictions. This is argued necessary due to the increasing adoption of Internet of Things (IOT) devices brings with it the inability to categories the future wireless devices that may require unlocking. Continuously requiring to amend this enumerated list of device in the face of unimaginable and fast paced change will consistently hinder this realm of technology.

b) The opposition's argument to allow for the jailbreaking of voice assistant devices centered around its increased capacity to infringe on copyright law via increased piracy. Jailbreaking these devices would allow a greater capacity to both allow for access to pirated content and counterfeit/copyrighted apps themselves. Unlike regular computing devices, voice assistants have reduced security options based on their computational simplicity. As a side, they also challenged the premise stated by the proponent: that jailbreaking devices aids in the development of new applications.

The exemption was granted in the entirety proposed by the proponents. The decision was based on the fact that the court found little evidence to suggest that the current exemption (such as jailbreaking smartphones or tablets) had any market harm to copyright infringement. The court holds that threats to copyright subscription based streaming services, although a serious issue, was not threatened moreso by voice based devices in comparison to those currently exempt. Further manipulation of device firmware had little means to infringe on streaming services' copyright as these platforms had security measures independent of the device and firmware itself.

A likely response from device manufacturers will be to void warranties on jail broken devices and attempt to identify such devices in order to remove their capable and connection to services and future updates.

c) The first hinderance to hacking into a hospital or hospital equipment is that good faith research must be conducted on devices that are not currently being used and will never be so. Secondly, there is restrictions in the clause so that access is granted *"where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public".* Clearly, an uninformed hopsital would not meet such a standard.

Programming Questions

Question 1

The last word oracle would (for a single pad bit) be expecting a 0 character rather than a 1. Thus in this case of a single padding word

$$C^{-1}(y) = r_b \oplus 1$$

Becomes:

$$C^{-1}(y) = r_b \oplus 0 = r_b$$

This propagates to step 5b in the padding oracle:

$$\ldots \textit{and output } (r_{b-n+1})(r_{b-n+2} \oplus n)\ldots(r_n \oplus n)$$

In section 3.2, step 5 is now expecting a zero padding word not a word of (b-j+2). Thus:

$$\textit{output } r_{j-1} \oplus i$$

Question 2

The same as the paper.

Question 6

Electronic Codebook mode (ECB) is not a valid means for providing security in web applications. It is also easily susceptible to padding oracle attacks. Because each block is encrpyted separately, inspection of a sequence can easily identify the padding scheme, and thus standard decryption means (that is, like above) can ensue. Considering that only the final block would have padding, comparison of this block to the second last block will detail the padding scheme. Further, comparison between different final blocks is all you'd need to ultimately understand the padding scheme. The attacks follow analogously to the CBC henceforth.