Brian Bauman

**CSC 435 - Assignment 7**

RSA Lab

3.1

The private key, d, is 182363E2DA763AD4DC94DBE64CD6869FEDD1B10B1E8810416A9CD4E9AF6B7FC5 (see calculateD.c for code).

3.2

The encrypted message, c, is 6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC (see encryptM.c for code).

3.3

The decrypted message, m, is password is dees (see decryptC.c for code)

3.4

The signature, S, is 55A4E7F17F04CCFE2766E1EB32ADDBA890BBE92A6FBE2D785ED6E73CCB35E4CB (see signM.c for code). When changing the message to “I owe you #$3000.”, the signature becomes BCC20FB7568E5D48E434C387C06A6025E90D29D848AF9C3EBAC0135D99305822. Even though it was a slight change, the signature is completely different.

3.5

The signature is indeed Alice’s as can be seen in verifyS.c, which outputs a value, in hex, of 4C61756E63682061206D6973736C652E, which matches the hex of the message “Launch a missile.”. By changing the 2F to 3F, we get a message that looks nothing like the original. In hex, it is 91471927C80DF1E42C154FB4638CE8BC726D3D66C83A4EB6B7BE0203B41AC294.

3.6

Step 1

The certificate from [www.google.com:443](http://www.google.com:443) is:

Certificate chain

0 s:/C=US/ST=California/L=Mountain View/O=Google LLC/CN=www.google.com

i:/C=US/O=Google Trust Services/CN=Google Internet Authority G3

-----BEGIN CERTIFICATE-----

MIIEgjCCA2qgAwIBAgIIaffBBSPuxFUwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UE

BhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczElMCMGA1UEAxMc

R29vZ2xlIEludGVybmV0IEF1dGhvcml0eSBHMzAeFw0xODA1MDgxNDQ5NTZaFw0x

ODA3MzExMzI3MDBaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlh

MRYwFAYDVQQHDA1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKDApHb29nbGUgTExDMRcw

FQYDVQQDDA53d3cuZ29vZ2xlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC

AQoCggEBAMUNse2GJhLm1LcVZtRP4uXxLxtwW+6/OiIhBASvf2rkw5aeoKxwkvu5

C3gSSeX9NRQ3HmgL5kcy2pAREn/dkyJndiBEaWievOkDMoMWCMxSRv5jCDiWRAEP

UHfmaEp8sX48oVEOUMBCzOzpFVjy4wLdSh5Jk/gZI9Ehgh0zbOyFu1mgsh9gYdtr

dyjk3eA6veN9t4glqOXrD+2JOkh9Ruv7JC3wG9mi7X3cpYINLcG4E1XBbAOa0b9o

U37a9NREAlWcEz/fF4rAh4BZsIPGTNxEEpi890y4nDXR9b2rTB2r2/+Hx0UM65Mm

nM499bwEVqj5VCr2aHISy6hJlK5WK6kCAwEAAaOCAUIwggE+MBMGA1UdJQQMMAoG

CCsGAQUFBwMBMBkGA1UdEQQSMBCCDnd3dy5nb29nbGUuY29tMGgGCCsGAQUFBwEB

BFwwWjAtBggrBgEFBQcwAoYhaHR0cDovL3BraS5nb29nL2dzcjIvR1RTR0lBRzMu

Y3J0MCkGCCsGAQUFBzABhh1odHRwOi8vb2NzcC5wa2kuZ29vZy9HVFNHSUFHMzAd

BgNVHQ4EFgQUwt/iKbjN4d4XzoJqVYZxA5MdFZYwDAYDVR0TAQH/BAIwADAfBgNV

HSMEGDAWgBR3wrhQmmd2drEtwobQg6B+pn66SzAhBgNVHSAEGjAYMAwGCisGAQQB

1nkCBQMwCAYGZ4EMAQICMDEGA1UdHwQqMCgwJqAkoCKGIGh0dHA6Ly9jcmwucGtp

Lmdvb2cvR1RTR0lBRzMuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQAlcV8MfHlBVAeq

u/VA3+kdhCFoDcnBur2SoBJycbAkk8KkEchfHme//TxGly9rlEBj8GcQrsPIVTm6

oZavEFmMGXAwsI92/3MQSjAIV+H1JH96SQ5tf8MaXJFSIT1Ge77Y0kGUdmpkNSaf

khW0VKIrUpdQgeum2MjJUxiw877EA5Xz3TrXrdOX5R1HC/HSKExLlvymxBPRUtB+

HX2rhCtk4YkUSrLXZG0+KN9Zu5S6CleCEzlJ+64N8OBHkSrAi1uyqiHpTqXHNgty

XHiB53drkRGQt0D6Ljdsf7cPfxUbWaNrDnl644vu5SHnbykP0/wpLZBC/Cvx/a1l

KDj15iQx

-----END CERTIFICATE-----

1 s:/C=US/O=Google Trust Services/CN=Google Internet Authority G3

i:/OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign

-----BEGIN CERTIFICATE-----

MIIEXDCCA0SgAwIBAgINAeOpMBz8cgY4P5pTHTANBgkqhkiG9w0BAQsFADBMMSAw

HgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEGA1UEChMKR2xvYmFs

U2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjAeFw0xNzA2MTUwMDAwNDJaFw0yMTEy

MTUwMDAwNDJaMFQxCzAJBgNVBAYTAlVTMR4wHAYDVQQKExVHb29nbGUgVHJ1c3Qg

U2VydmljZXMxJTAjBgNVBAMTHEdvb2dsZSBJbnRlcm5ldCBBdXRob3JpdHkgRzMw

ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDKUkvqHv/OJGuo2nIYaNVW

XQ5IWi01CXZaz6TIHLGp/lOJ+600/4hbn7vn6AAB3DVzdQOts7G5pH0rJnnOFUAK

71G4nzKMfHCGUksW/mona+Y2emJQ2N+aicwJKetPKRSIgAuPOB6Aahh8Hb2XO3h9

RUk2T0HNouB2VzxoMXlkyW7XUR5mw6JkLHnA52XDVoRTWkNty5oCINLvGmnRsJ1z

ouAqYGVQMc/7sy+/EYhALrVJEA8KbtyX+r8snwU5C1hUrwaW6MWOARa8qBpNQcWT

kaIeoYvy/sGIJEmjR0vFEwHdp1cSaWIr6/4g72n7OqXwfinu7ZYW97EfoOSQJeAz

AgMBAAGjggEzMIIBLzAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0lBBYwFAYIKwYBBQUH

AwEGCCsGAQUFBwMCMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFHfCuFCa

Z3Z2sS3ChtCDoH6mfrpLMB8GA1UdIwQYMBaAFJviB1dnHB7AagbeWbSaLd/cGYYu

MDUGCCsGAQUFBwEBBCkwJzAlBggrBgEFBQcwAYYZaHR0cDovL29jc3AucGtpLmdv

b2cvZ3NyMjAyBgNVHR8EKzApMCegJaAjhiFodHRwOi8vY3JsLnBraS5nb29nL2dz

cjIvZ3NyMi5jcmwwPwYDVR0gBDgwNjA0BgZngQwBAgIwKjAoBggrBgEFBQcCARYc

aHR0cHM6Ly9wa2kuZ29vZy9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEA

HLeJluRT7bvs26gyAZ8so81trUISd7O45skDUmAge1cnxhG1P2cNmSxbWsoiCt2e

ux9LSD+PAj2LIYRFHW31/6xoic1k4tbWXkDCjir37xTTNqRAMPUyFRWSdvt+nlPq

wnb8Oa2I/maSJukcxDjNSfpDh/Bd1lZNgdd/8cLdsE3+wypufJ9uXO1iQpnh9zbu

FIwsIONGl1p3A8CgxkqI/UAih3JaGOqcpcdaCIzkBaR9uYQ1X4k2Vg5APRLouzVy

7a8IVk6wuy6pm+T7HT4LY8ibS5FEZlfAFLSW8NwsVz9SBK2Vqn1N0PIMn5xA6NZV

c7o835DLAFshEWfC7TIe3g==

-----END CERTIFICATE——

Step 2

The value of n isand the value of e is 65537.

Step 3

The signature is .

Step 4

The hash of the signature is d0266b90257c91cd912daa5aa11374803041396c6863aa58eefcbe29c735834b.

Step 5

Running the command openssl verify c1.pem returned a value of c1.pem: OK.

Secret Key Lab

2.1

The encrypted message is:

THE OSCARS TURN ON SUNDAY WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE

AWARDS TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO

THE AWARDS RACE WAS BOOKENDED BY THE DEMISE OF HARVEY WEINSTEIN AT ITS OUTSET

AND THE APPARENT IMPLOSION OF HIS FILM COMPANY AT THE END AND IT WAS SHAPED BY

THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVISM AND

A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE

OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT JUST SEEM EXTRA LONG IT WAS

EXTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MARCH TO

AVOID CONFLICTING WITH THE CLOSING CEREMONY OF THE WINTER OLYMPICS THANKS

PYEONGCHANG

ONE BIG QUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE

CEREMONY WILL ADDRESS METOO ESPECIALLY AFTER THE GOLDEN GLOBES WHICH BECAME

A JUBILANT COMINGOUT PARTY FOR TIMES UP THE MOVEMENT SPEARHEADED BY

POWERFUL HOLLYWOOD WOMEN WHO HELPED RAISE MILLIONS OF DOLLARS TO FIGHT SEXUAL

HARASSMENT AROUND THE COUNTRY

SIGNALING THEIR SUPPORT GOLDEN GLOBES ATTENDEES SWATHED THEMSELVES IN BLACK

SPORTED LAPEL PINS AND SOUNDED OFF ABOUT SEXIST POWER IMBALANCES FROM THE RED

CARPET AND THE STAGE ON THE AIR E WAS CALLED OUT ABOUT PAY INEQUITY AFTER

ITS FORMER ANCHOR CATT SADLER QUIT ONCE SHE LEARNED THAT SHE WAS MAKING FAR

LESS THAN A MALE COHOST AND DURING THE CEREMONY NATALIE PORTMAN TOOK A BLUNT

AND SATISFYING DIG AT THE ALLMALE ROSTER OF NOMINATED DIRECTORS HOW COULD

THAT BE TOPPED

AS IT TURNS OUT AT LEAST IN TERMS OF THE OSCARS IT PROBABLY WONT BE

WOMEN INVOLVED IN TIMES UP SAID THAT ALTHOUGH THE GLOBES SIGNIFIED THE

INITIATIVES LAUNCH THEY NEVER INTENDED IT TO BE JUST AN AWARDS SEASON

CAMPAIGN OR ONE THAT BECAME ASSOCIATED ONLY WITH REDCARPET ACTIONS INSTEAD

A SPOKESWOMAN SAID THE GROUP IS WORKING BEHIND CLOSED DOORS AND HAS SINCE

AMASSED MILLION FOR ITS LEGAL DEFENSE FUND WHICH AFTER THE GLOBES WAS

FLOODED WITH THOUSANDS OF DONATIONS OF OR LESS FROM PEOPLE IN SOME

COUNTRIES

NO CALL TO WEAR BLACK GOWNS WENT OUT IN ADVANCE OF THE OSCARS THOUGH THE

MOVEMENT WILL ALMOST CERTAINLY BE REFERENCED BEFORE AND DURING THE CEREMONY

ESPECIALLY SINCE VOCAL METOO SUPPORTERS LIKE ASHLEY JUDD LAURA DERN AND

NICOLE KIDMAN ARE SCHEDULED PRESENTERS

ANOTHER FEATURE OF THIS SEASON NO ONE REALLY KNOWS WHO IS GOING TO WIN BEST

PICTURE ARGUABLY THIS HAPPENS A LOT OF THE TIME INARGUABLY THE NAILBITER

NARRATIVE ONLY SERVES THE AWARDS HYPE MACHINE BUT OFTEN THE PEOPLE FORECASTING

THE RACE SOCALLED OSCAROLOGISTS CAN MAKE ONLY EDUCATED GUESSES

THE WAY THE ACADEMY TABULATES THE BIG WINNER DOESNT HELP IN EVERY OTHER

CATEGORY THE NOMINEE WITH THE MOST VOTES WINS BUT IN THE BEST PICTURE

CATEGORY VOTERS ARE ASKED TO LIST THEIR TOP MOVIES IN PREFERENTIAL ORDER IF A

MOVIE GETS MORE THAN PERCENT OF THE FIRSTPLACE VOTES IT WINS WHEN NO

MOVIE MANAGES THAT THE ONE WITH THE FEWEST FIRSTPLACE VOTES IS ELIMINATED AND

ITS VOTES ARE REDISTRIBUTED TO THE MOVIES THAT GARNERED THE ELIMINATED BALLOTS

SECONDPLACE VOTES AND THIS CONTINUES UNTIL A WINNER EMERGES

IT IS ALL TERRIBLY CONFUSING BUT APPARENTLY THE CONSENSUS FAVORITE COMES OUT

AHEAD IN THE END THIS MEANS THAT ENDOFSEASON AWARDS CHATTER INVARIABLY

INVOLVES TORTURED SPECULATION ABOUT WHICH FILM WOULD MOST LIKELY BE VOTERS

SECOND OR THIRD FAVORITE AND THEN EQUALLY TORTURED CONCLUSIONS ABOUT WHICH

FILM MIGHT PREVAIL

IN IT WAS A TOSSUP BETWEEN BOYHOOD AND THE EVENTUAL WINNER BIRDMAN

IN WITH LOTS OF EXPERTS BETTING ON THE REVENANT OR THE BIG SHORT THE

PRIwE WENT TO SPOTLIGHT LAST YEAR NEARLY ALL THE FORECASTERS DECLARED LA

LA LAND THE PRESUMPTIVE WINNER AND FOR TWO AND A HALF MINUTES THEY WERE

CORRECT BEFORE AN ENVELOPE SNAFU WAS REVEALED AND THE RIGHTFUL WINNER

MOONLIGHT WAS CROWNED

THIS YEAR AWARDS WATCHERS ARE UNEQUALLY DIVIDED BETWEEN THREE BILLBOARDS

OUTSIDE EBBING MISSOURI THE FAVORITE AND THE SHAPE OF WATER WHICH IS

THE BAGGERS PREDICTION WITH A FEW FORECASTING A HAIL MARY WIN FOR GET OUT

BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE

SHAPE OF WATER HAS NOMINATIONS MORE THAN ANY OTHER FILM AND WAS ALSO

NAMED THE YEARS BEST BY THE PRODUCERS AND DIRECTORS GUILDS YET IT WAS NOT

NOMINATED FOR A SCREEN ACTORS GUILD AWARD FOR BEST ENSEMBLE AND NO FILM HAS

WON BEST PICTURE WITHOUT PREVIOUSLY LANDING AT LEAST THE ACTORS NOMINATION

SINCE BRAVEHEART IN THIS YEAR THE BEST ENSEMBLE SAG ENDED UP GOING TO

THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE ACTORS MAKE UP THE ACADEMYS

LARGEST BRANCH THAT FILM WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE

AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST

DIRECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO

EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN

This message uses the following cipher:

y -> T

t -> H

n -> E

m -> I

u -> N

v -> A

q -> S

p -> D

x -> O

z -> U

h -> R

b -> F

l -> W

r -> G

f -> V

a -> C

d -> Y

e -> P

c -> M

i -> L

k -> X

g -> B

s -> K

j -> Q

o -> J

w -> Z

2.2

By entering the command openssl enc -aes-128-cbc -e -in plain.txt -oun -K 00112233445566778889aabbccddeeff -iv 0102030405060708, we are able to encrypt the plain text above (see cipher.bin).

2.3

I encrypted the picture by entering openssl enc -aes-128-cbc -e -in pic\_original.bmp -out p2.bmp -K 00112233445566778889aabbccddeeff -iv 0102030405060708, creating p2.bmp (see p2.bmp). Swapping the headers, new.bmp was created (see new.bmp), which looks like:

Repeating this process for a picture of my own had similar results.

2.4.1

I chose to encrypt the pic\_original.bmp file from the previous steps. The original file size was 184,974 bytes. After encryption, the file sizes were as follows:

- AES 128 bit ECB: 184,976 bytes (requires padding)

- AES 128 bit CBC: 184,976 bytes (requires padding)

- AES 128 bit CFB: 184,974 bytes (does not require padding)

- AES 128 bit OFB: 184,974 bytes (does not require padding)

The methods that do not require padding effectively treat the block cipher as a stream cipher. From Wikipedia:

CFB, OFB and CTR modes do not require any special measures to handle messages whose lengths are not multiples of the block size, since the modes work by [XORing](https://en.wikipedia.org/wiki/Exclusive_or) the plaintext with the output of the block cipher. The last partial block of plaintext is XORed with the first few bytes of the last [keystream](https://en.wikipedia.org/wiki/Keystream) block, producing a final ciphertext block that is the same size as the final partial plaintext block.

(See pic\_aes128[cipher].bmp for encrypted output.)

2.4.2

The size of the files is as follows:

dummy10bytes.txt: 10 bytes

dummy10bytes-aes128cbc.txt: 16 bytes

dummy16bytes.txt: 16 bytes

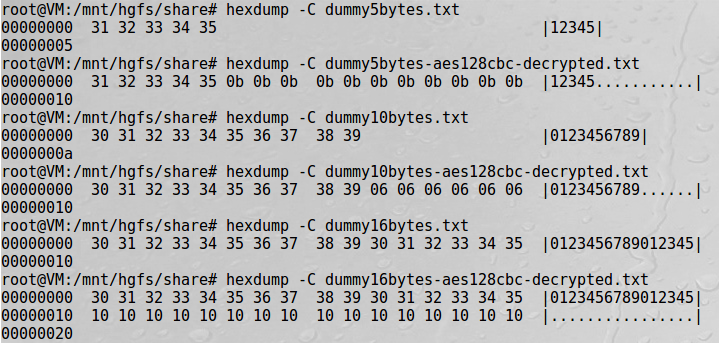
dummy16bytes-aes128cbc.txt: 32 bytes

dummy5bytes.txt: 5 bytes

dummy5bytes-aes128cbc.txt: 16 bytes

(See submission for file examples.)

After decrypting the files with -nopad, we can see that they are padded. Below is a screenshot of the hex dump, but the output files are also included in the submission (see dummy[size]bytes-aes128-cbc-decrypted.txt).



2.5

My guess is that none of the files will have recoverable data after editing a single byte of the encrypted file, regardless of the encryption method.

(See dummy1000bytes-aes128[method].txt for the modified encrypted files.)

After decrypting the modified files, they were all very recoverable. The OFB file had only the relevant byte messed up. The other files had only the local bytes messed up. In all cases, the majority of the file was recoverable even after the decrypted file was slightly modified.

(See dummy1000bytes-aes128[method]-decrypted.txt for the decrypted versions of the modified encrypted files.)

Because OFB performs identical operations in the encryption and decryption process (per <https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Output_Feedback_(OFB))>, it makes sense that reversing the process would only result in a single malformed byte.

2.6.1

When using the same IV, the resulting encrypted ciphertext is identical. Using a different IV produces a new ciphertext (see test.txt, test-aes128cbc.txt, and test-aes128cbc-2.txt). As such, uniqueness is important because it guarantees that the same (encrypted) messages sent twice will not be identifiable as identical, preventing malicious third parties from detecting patterns or gleaning information from the network.

2.6.2

Because CFB uses the ciphertext as the initialization vector for each subsequent block, it would be impossible to glean information from a given ciphertext in this scenario unless the blocks were repeating themselves in someway. OFB, on the other hand, uses the plaintext each time, which means that having one plaintext/ciphertext pair is much more useful.

2.6.3

This mode of attack is problematic because if you can predict the next initialization vector, you can choose a particular plain-text, watch it be encrypted, and determine whether or not it matches the ciphertext produced by the previous initialization vector. If the guess is correct, the resultant ciphertext will be equivalent to the original ciphertext. (See <https://en.wikipedia.org/wiki/Initialization_vector#Properties> for further details.)