Week 2 - Number Theory Basics and the One-Time Pad

MAT260: Cryptology

Gary Hobson

May 13, 2015

Introduction:

The assigned computer problems this week are from Chapter 3, Problems 1, 6, 7, and Chapter 4, Problems 2, 4.

Make sure to review the example computer problems in "Appendix C.3 Examples for Chapter 3" that work similar problems to those you are assigned.

Make sure to run your code so all relevant computations/results are displayed and then export your work as a PDF file for submission.

Chapter 3 Problems:

Problem 1:

```
a = 8765;
b = 23485;

g = gcd(a, b);
disp(['gcd(', num2str(a), ', ', num2str(b), ') = ', num2str(g)]);
```

```
gcd(8765, 23485) = 5
```

Problem 6:

```
% Given values
a = 314;
b = 271;
n = 11111;

% find the mod inverse
a_inv = invmodn(a, n);

% find the solution
x = mod(a_inv * b, n);

disp(['x ≡ ', num2str(x), ' mod ', num2str(n)]);
```

```
x ≡ 10298 mod 11111
```

Problem 7:

```
a = 216;
b = 66;
n = 606;

% find gcd
d = gcd(a, n);

% Simplify
a1 = a / d;
b1 = b / d;
n1 = n / d;

% Find inverse of a1 mod n1
a1_inv = invmodn(a1, n1);

% Find the base solution
x0 = mod(a1_inv * b1, n1);

% Genterate all d solutions
solutions = zeros(1, d);
for k = 0:d-1
    solutions(k+1) = mod(x0 + k * n1, n);
end
disp(solutions);
```

```
    48   149   250   351   452   553
```

Chapter 4 Problems:

Problem 2:

```
filename = 'words.txt';  % i found this list online
fid = fopen(filename, 'r');

raw = textscan(fid, '%s');
fclose(fid);

% Filter dictionary to 5 letter words
dictionary = lower(raw{1});
dictionary = dictionary(cellfun(@length, dictionary) == 5);

ciphertext = 'evire';

% Loop through all shifts and find matches
valid_candidates = {};
for j = 0:25
    candidate = shift(ciphertext, -j);
    if ismember(candidate, dictionary)
        valid_candidates{end+1} = candidate;
    end
end
disp(valid_candidates);
```

```
    {'arena'}    {'river'}
```

```

% find probability
if any(strcmp(valid_candidates, 'arena'))
    p = 1 / length(valid_candidates);
    fprintf('P(M = "arena" | C = "evire") = %.2f\n', p);
else
    disp('"arena" is not a valid message');
end
```

```
P(M = "arena" | C = "evire") = 0.50
```

Problem 4:

```
filename = 'words.txt';
fid = fopen(filename, 'r');
if fid == -1
    error('words.txt not found.');
end
raw = textscan(fid, '%s');
fclose(fid);

% Filter dictionary to 6 letter words
dictionary = lower(raw{1});
dictionary = dictionary(cellfun(@length, dictionary) == 6);

% Ciphertext to analyze
ciphertext = 'eblkfg';
%n = length(ciphertext);

% Initialize list of valid messages
valid_messages = {};

% Loop through all words
for i = 1:length(dictionary)
    m = dictionary{i};
    key = mod(double(ciphertext) - double(m), 26);

    % Check if the key is periodic with period 3
    if isequal(key(1:3), key(4:6))
        valid_messages{end+1} = m;
    end
end
```

```
disp(valid_messages');
```

```
    {'failed'}
    {'gasmen'}
    {'hained'}
    {'laired'}
    {'messin'}
    {'sawyer'}
    {'unpark'}
```

```

% Calculate probabiliyt
if any(strcmp(valid_messages, 'attack'))
    p = 1 / length(valid_messages);
    fprintf('P(M = "attack" | C = "eblkfg") = %.2f\n', p);
else
    fprintf('"attack" is not a valid messages for ciphertext "eblkfg"\n');
end
```

```
"attack" is not a valid messages for ciphertext "eblkfg"
```