Cryptography and Network Security Assignment 1.

Lecturer: Damien Fay. Room 104, St. Declans. Ext: 2320.

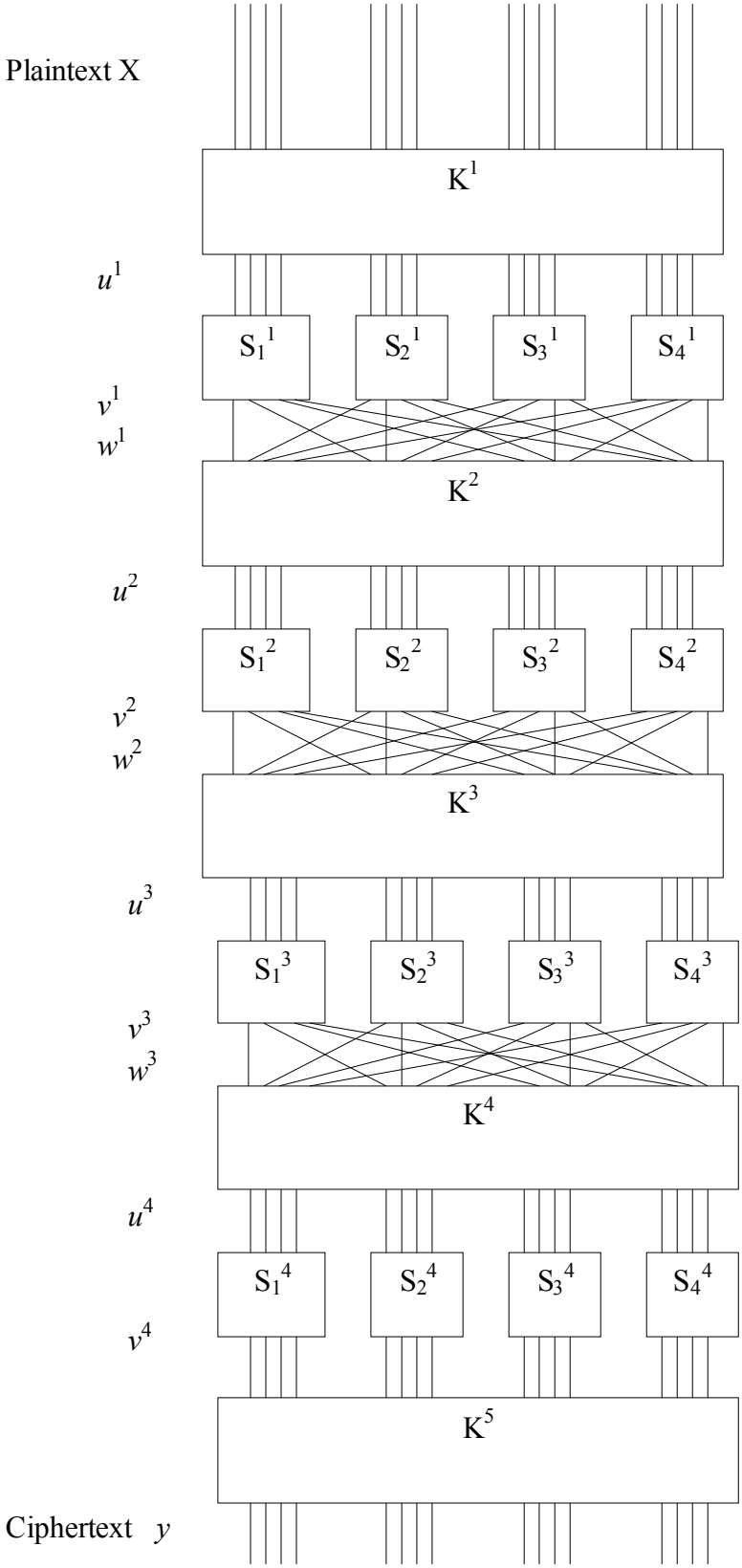
Submission date: 5pm - Fri 12th November 2004. Note: 5% will be deducted from total possible mark for each day late.

Objectives: To understand and implement a linear cryptographic attack on a simple SPN. Statistical analysis of results. An introduction to academic paper formats and writing.

Marks: This assignment counts for the equivalent of 15% of your overall mark for this subject.

Assignment I. Part I:

Construct the following cryptographic algorithm in matlab using functional blocks. The algorithm should be able to produce *N*-rounds with arbitrary s-boxes:



Where the following are defined:

K^i: $w^i \oplus k_1$ i.e. just a bit wise XOR operation. Where k_i is sub-key i.

e.g.:

w = 0010 0110 1011 0111
k = 0011 1010 1001 0100
u = 0001 1100 0010 0011 Note: u is the output.

S^1: $u \rightarrow$ v : A substitution formed using the following table:

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
v	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

E.g.

u = 0001 1100 0010 0011 in Hex: 1 C 2 3
v = 0100 0101 1101 0001 4 5 D 1

P^1: v $\rightarrow$ w : A Permutation formed using the following table (bit numbers):

v	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
w	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

E.g.

v= 0100 0101 1101 0001

w = 0010 1110 0000 0111

Note: for simplicity all the s-boxes are the same. i.e. $S_1^2 = S_1^1$ etc.

Sub-key generation:

The sub-key generation algorithm takes the following:

A 32 bit key, k, is taken as input and consecutive parts are taken as the key.

e.g.

K = 0011 1010 1001 0100 1101 0110 0011 1111

k^1= 0011 1010 1001 0100
k^2= 1010 1001 0100 1101
k^3= 1001 0100 1101 0110
k^4= 0100 1101 0110 0011
k^5= 1101 0110 0011 1111

Finally, as a check given the following key and plaintext you should produce the following cipertext:
x = 0010 0110 1011 0111
K = 0011 1010 1001 0100 1101 0110 0011 1111
y = 1011 1100 1101 0110

Part II:

Construct the linearization table for the S-boxes and analyse this SPN using a linear attack.

Part III: Report

The report should follow the format of the paper which will be forwarded to you or which can be found at the following html address:

http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V0F-3TK6JGD-6-2&_cdi=5645&_orig=search&_coverDate=06%2F30%2F1998&_sk=999339993&view=c&wchp=dGLbVzb-zSkWz&_acct=C000007922&_version=1&_userid=103680&md5=a895806d4f49479d9c4d130ab538a9c8&ie=f.pdf

Do not worry about the actual contents of the paper; it's the format which is important. Academic papers are laid out in **a *very specific*** format. This is so people who read them regularly, know where to find what they're looking for quickly, can get a quick impression of the subject matter and can trace previous research in the subject. It is a well worthwhile exercise to become familiar with this as it allows you to present information in a way that is widely accepted by everyone.

Also if someone reads a paper that has haphazard or original formatting then they quickly get lost and abandon the paper.

Specifically, the report should contain the following elements:

1. **Abstract**. At most 100 words which describe concisely what the paper is about and what the main result is.

2. **Introduction** (no more than ½ page). Give a bit of background and what the aim is.

3. **The SPN network**. Description of the SPN without going into huge amount of detail.

4. **Implementation**. Any details about how you implemented the algorithms: e.g. How the keys where generated or anything else you can think of. Any problems attacking etc. and how you overcame them (or not!). Don't put anything in about how your code is written or a listing.

5. **Results**. The analysis of the attack. This is the part where you can add extra statistical analysis of the attack not expressly done in the assignment.

6. **Conclusion**. You can be brief here. Take space if you need to talk about an important result but don't waffle.

7. **References**. List all the references that you used. There will only be a few but be sure that it is indicated in the text (numbered e.g. [3]) where you read this or that bit. Remember if a large set of text is unreferenced then it's something **you're claiming to have discovered yourself**!!!. On the other hand don't have every line referenced look at the paper and see how he strikes a balance.

Part IV: Deliverables.

A **paper** copy of the report. A copy of the report and m-files via e-mail (no disks please).