Symmetric Crypto

Decrypt equation: Pi= D_K(C-i XOR Ci)

1) It is easy to calculate E(K,Pi) because IV is known and Ci-1 is the previous message sent.

E(K,Pi) = ci XOR to ci-1

Then this method has the same weakness as ECB in that we can see if two plaintext blocks are the same.

2) It is also now easy to reorder the blocks E(K,Pi).

For example C'1= IV XOR E(K,P2), C'2 = C'1 XOR E(K,P3), C'3= C'2 XOR E(K,P1)

Integrity

One: In approach 1 Bob ends up with H(M) so there is now way for him to know what M is. So this approach fails in its basic purpose to send a message to Bob. And since Bob does not know the message there is by implication also no message authentication.

Two: If you find a collision on MD5 then there will also be a collision on SHA (as the inputs to SHA would be the same value – so the collision effort is 2^ (128/2) = 2^64

Authentication/Key Management

Yours is correct. There are many examples, you can also use timestamps…

Method 1

```
> N

< D(N)
```

Method 2

```
> N

< E(N)
```

Method 3

```
> E(N)

< N
```

Method 4

```
> N

< MAC(N)
```

Network Security

One

SRES is 32 bits and RAND is 128 bits. The reason is that RAND should not repeat so the number is very large. For SRES it needs to be large enough so the probability of an attacker guessing it is low. At the moment the chance of guessing SRES correctly is 2^-32. You have a single guess, so you have 1 out of the total possibility chance to be right.

Computer Security

The key question here is does each approach give us the ideal security gain provided by a salted hash password file. In other words, does the attacker need to build a dictionary larger than the number of possible passwords.

i. OK

ii. OK

iii. Not OK. We know s and therefore h(s) so we are left searching for h(password) like unsalted case.

iv. Not OK. We can just decrypt the password because s is the key.

v. OK

vi. No OK. We can just decrypt the h(password) because s is the key, and then again it is searching the unsalted case.

vii. Ok. This is not really any different to i h (s, pwd). If it is hash (s’,h(s,pwd)) then you still need to build dictionary all values of s and pwd.

viii. Ok.