# TTM4137 Exam Dec. 12, 2011 Solution Outline

Stig F. Mjølsnes, Revised Dec. 19, 2011

## Part I. Wireless Networks Security Facts

1b, 2a, 3a, 4a, 5c, 6c, 7d, 8a, 9c, 10c, 11a, 12b, 13d, 14c, 15c, 16b, 17a, 18c, 19c, 20b, 21d, 22a, 23d, 24d, 25a.

## Part II. Cryptographic Mechanisms

26. A streamcipher does a bit-by-bit encryption process, whereas a block cipher does encryption of a whole block of bits. However, the RC4 cipher shows that this stream cipher operates on a byte by byte basis. A byte is a block of bits. Hence, we might consider a stream cipher a special case of a block cipher. On the other hand, we might consider a block cipher a special case of a stream cipher, observing that the block cipher keystream is constant. A stream cipher is an approximation of a Vernam one-time cipher. A block cipher is an approximation of a one-way function.

27. A one-way function is a function for which it is computationally 'easy to compute' the function value $f(x)$ given $x$, but no 'easy to compute' algorithm is known that outputs an $x'$, given a function value $y = f(x')$. 'Easy to compute' means a polynomial time algorithm with respect to the length of the input. More elaborate definitions exist.

28. $c_i = e_k(c_{i-1} \oplus m_i), i = \{1, 2, \ldots\}, c_0 = IV$.

29. The idea of a message authentication code (MAC), also called a message integrity code (MIC), or simply an authentication code, is to compute a check value by some algorithm with input the cryptographic key and all bits of the message, and send the resulting output value along with the message. The recipient will do the same computation and check that the output is equal to the received value. One example construction is the CBC-MAC variant of UIA f9, a cipher-block-chaining mode of operation.

30. The MD5 does not need a secret key input. There might be other reasons.

31. The purpose of the initialization vector is to change the cipher function even though the key is kept fixed. The same input will (very likely) result in a different output for each initialization vector value. The IV must never be reused with the same key because this opens for a replay attack, therefore the size of the IV set must be sufficiently large to avoid this reuse. The IV value can be chosen sequentially and is normally sent in the clear to the recipient. If the IV must be a non-predictable value, it must be selected by a (pseudo)random process.

32. The key space will depend on the `keyinput` length $k, 1 \geq k \leq 256$ bytes. The key space becomes $2^{8 \cdot k}$. Typical key length will be 16 bytes = 128 bits or 32 bytes = 256 bits. We do not require the student to compute the decimal representation of these integers, but here they are: The key space for 128 and 256 bit lengths are
340282366920938463463374607431768211456 (39 digits)
115792089237316195423570985008687907853269984665640564039457584007913129639936 (78 digits)
The full key length of RC4 is 256 bytes, or 2048 bits, and the key space for this is $256^{256}$
32317006071311007300714876688669951960444102669715484032130345427524

65513886789089319720141152291346368871796092189801949411955915049092
10950881523864482831206308773673009960917501977503896521067960576383
84067568276792218642619756161838094338476170470581645852036305042887
57589154106580860755239912393038552191433338966834242068497478656456
94948561760353263220580778056593310261927084603141502585928641771167
25943603718461857357598351152301645904403697613233287231227125684710
82020972515710172693132346967854258065669793504599726835299863821552
51663894373355436021354332296046453184786049521481935558536110595962
30656 (617 digits)

33. 256 possible values of `i`, and 256 possible values of `j`, and 256! possible permutations of the values 0-255 in `S[]`
hence $256 \cdot 256 \cdot 256!$ possible states. This number has 512 digits, not required to compute this:
56217945724868536180348175756901261322340369713036369583122392703124
73084252308041743992693459854350420383402179537038908831805175848609
22067215508109673120189407122268729367883071624070296082964787277313
81609647813563352786301843191181300603344183382881259944723983353869
38050153827654752634923044950884227942008865157673628382230385215000
66962607462650221834312549140798559454555997436272383820907785920748
98228095381341656904118528142515629981696000000000000000000000000000
000000000000000000000000000000000000
Ideally, the number of states of the generator should be approximately the same as the key space. If the key space is larger than the number of states, then many keys will collide to the same state. The cross-over for $k$ is where $256^{k-2} \approx 256!$.

## Part III. Protocols

34. The attacker categories and the granularity of these may vary. For instance, in increasing capability order:
Passive (readonly), Active (Modify message, Initiator, Responder, Man-in-the-middle with several sessions, ...), Insider games, Insider collusions.
35. This problem is open for many ingenious solutions. One solution is given in slide 15 of the Lecture Notes 13, Nov. 11, 2011. RFC3329

—