December 20, 2021, Midterm 2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q1: Describe how forward secrecy can be accomplished even when using a pre-shared key – in such description clarify into details how session keys can be technically computed (which quantities, functions, etc)

Q2: Which of the following TLS related statements are true (T), false (F) or not applicable (NA) when the question is ill-posed or does not make sense *(comments can be added on the right if/when necessary)*

Unlike previous versions, TLSv1.2 supports only block ciphers	**T F NA**
When using TLS in ESP mode, both encryption and payload integrity are guaranteed	**T F NA**
DTLS explicitly transmits sequence numbers whereas TLS does not	**T F NA**
In the certificate transparency framework, a revoked TLS certificate is removed from the CT database	**T F NA**
TLS permits either single as well as mutual authentication	**T F NA**
In a TLS renegotiation, a same TLS session covers multiple TCP connections	**T F NA**
When using CBC, the BEAST attack is also feasible if the IV repeats	**T F NA**
Until TLS1.2, the FINISHED message was transmitted before the change cipher spec message	**T F NA**
When using fixed Diffie-Hellman, when connecting to a same server, the Master Secret always computes to the same value.	**T F NA**

Q3: Assuming a 4-bit block cipher based on the specific permutation given in the below table on the left,

1. Illustrate the CBC and CTR constructions, commenting on the parallelizability of operations in encryption and/or decryption.
2. Using CBC, decrypt the plaintext (1100) 1000.0011.0101 - (1100 is the initialization vector)
3. Using CTR, decrypt the plaintext (1100) 1000.0011.0101 - (1100 is the initial counter block)

input	output
0000	0001
0001	0010
0010	1011
0011	1111
0100	1101
0101	0000
0110	0011
0111	1001
1000	0110
1001	1000
1010	0101
1011	0111
1100	1110
1101	1100
1110	1010
1111	0100

Q4: Multiple answer questions:

In Ipsec IKE, a Stateless Cookie is	A cookie which can be verified without any secret key	A cookie which can be verified without storing it in the server memory	A cookie which can be verified without being first transmitted	A cookie which has no State but can be used in any region of the world
in IPsec ESP tunnel mode:	both inner and outer IP headers are protected	Only the outer IP header is protected	Only the inner IP header is protected	Neither outer nor inner IP headers are protected, only IP payload is
Is there a security problem when using 0-RTT in TLS1.3?	No. It is as secure as any other TLSv1.3 feature	Yes, it may permit a MITM attack	Yes, it may permit to replay previously sent application data	Yes, it may permit to impersonate the server
When using TSL_DHE_RSA_WITH_xxx,	Server can select wether to use DH or RSA for key management	Server must use both DH and RSA for key transport	the DH coefficients are signed by a CA using an RSA signature	the DH coefficients are signed by the client/server using an RSA signature
How many mult/squares are needed to compute g^17 mod p?	4	5	8	16
Which block cipher mode among those is NOT semantically secure?	OFB	CBC	ECB	CTR

Q5: Using **Modulo 85**, compute the following modular inverses, explaining which of those are trivial and which of those (if any) cannot be computed and why; In addition, for case (3), show step-by-step how you do apply the Extended Euclidean Algorithm.

1) 84^{-1} mod 85 =…

2) 80^{-1} mod 85 =…

3) 78^{-1} mod 85 =…

Q6: Consider a "vanilla" (i.e., no padding) RSA construction using modulo n=330.481 and public key e=3. Assume you see the ciphertext CT = 294.975, and assume you know that this ciphertext encrypts message M = 1000. Show, first in theory and then by computing the actual numerical values, which new ciphertext CT2 should be delivered to the receiver so that the internal message gets modified to the value M2 = 1003.

> [if you need to compute inverse values modulo n, here are a few modular inversions that may or may not be useful for solving this exercise – if you need more please use the extended GCD:
> {2, 3, 10, 100, 103, 1000, 1003} → {165241, 220321, 297433, 261080, 179679, 26108, 22076}]

Q7 – open discussion question - Alice and Bob have recently joined the IETF (Internet Engineering Task Force) in order to revise the current state of the TLS standard by working on an alternative version, X-TLS. During their years at university, they have learned that complexity is a problem when it comes to security. Said in another way "less is more". Striving to simplify the TLS protocol, Alice and Bob propose a drastic change: remove all things related to certificates from the TLS protocol.

Is this drastic change the fruit of naivety and inexperience, or does it makes sense in some scenarios/settings? Argue, as if you were another member of the IETF committee, the pros and the cons of the described proposal, specifically discussing possible application scenarios (eventually none).

Q8. (TLS Padding Oracle Attack) – Assume a CBC-based block encryption scheme which uses block sizes of 4 bytes each. Assume that the attacker sees the following ciphertext comprising 6 blocks (hex notation):

f1 aa bb cc || 34 35 f9 9f || 01 02 10 20 || <u>11 12 13 14</u> || 65 66 11 11 || ff f0 00 10

Assume now that the server is vulnerable to a Padding Oracle attack, and assume that the fourth block (the one underlined) contains a secret code which is one among the following four passwords:

01 01 01 99 – 02 02 01 99 – 03 01 02 99 - 04 02 02 99

How many messages should the attacker send to the server/oracle to as to decrypt the secret code? And which specific modified ciphertext(s) shall the attacker send?