Ans 1.
이 프로토콜을 사용하기 위한 전제조건으로는, A와 B는 서로 인증이 된 상태 즉, 서로의 인증서를 받아 확인한 상태이며 서로의 공개키를 알고 있어야한다는 것 이다.
이 메시지를 받은 B가 해야할 일은,
1. M을 K1을 사용하여 복호화 한다.
2. 복호화된 C를 MAC.K2(C)를 사용하여 인증한다.
3. C에서 추출한 TA, K, KB를 사용하여 TA||K를 생성한다.
4. A의 공개키를 사용하여 M과 TA||K를 암호화한다.
5. 암호화된 메시지를 A에게 보내기 전에, 무작위 데이터를 생성하여 그 값을 KB로 암호화한다.
6. 암호화된 메시지와 암호화된 무작위 데이터를 A에게 보낸다.

Ans 2.

$3^2 \equiv 3 \times 3 \equiv 3 + 3 \equiv 0 (\mathrm{mod}\, 6)$
$3^4 \equiv (3^2)^2 \equiv 0^2 \equiv 0 (\mathrm{mod}\, 6)$
$3^8 \equiv (3^4)^2 \equiv 0^2 \equiv 0 (\mathrm{mod}\, 6)$
$3^{16} \equiv (3^8)^2 \equiv 0^2 \equiv 0 (\mathrm{mod}\, 6)$
$3^{32} \equiv (3^{16})^2 \equiv 0^2 \equiv 0 (\mathrm{mod}\, 6)$
$3^{64} \equiv (3^{32})^2 \equiv 0^2 \equiv 0 (\mathrm{mod}\, 6)$

$3^{80} \equiv (3^{64}) \times (3^{16}) \equiv 0 \times 0 = 0 (\mathrm{mod}\, 6)$

Ans 3.
먼저 2와 11의 최대공약수를 구하면, 1이다.
2의 역원을 찾기 위해서는 2x + 11y = 1을 만족하는 정수 x와 y를 찾아야한다. 이 식을 만족하는 정수 쌍은 (-5, 1)이 있다. 이때, 음수는 11을 더함으로써 양수로 표현할 수 있기 때문에 (6, 1)로도 쓸 수 있다. 따라서 2의 역원은 6이다.

Ans 4.
K1: KAB를 이용하여 A와 B가 통신하는 세션 키
K2, K3: A와 B가 상호 인증을 수행하기 위해 사용하는 키
K4: B가 A에게 보내는 메시지를 암호화하기 위한 키
K5: B가 A에게 보내는 메시지의 무결성을 보호하기 위한 키

KAB는 여러 세션키와 인증키를 생성하는데 사용되는데, KAB가 노출될 경우 모든 키가 노출되기 때문에 새로운 KAB를 생성하여 다시 새로운 세션키와 인증키들을 생성해야한다.