Review

Saturday, October 21, 2023 12:46 PM

Quiz 1(M)

3.

a. Vigenère with an eight-letter key word.

26^8

$26 \cdot 26$

Ⓐ Ⓑ ○○○○○○

b. Hill cipher where the plaintext is given in a 5x6 matrix.

$P \cdot K$

$(5 \times 6)(6 \times 6)$

26^{36}

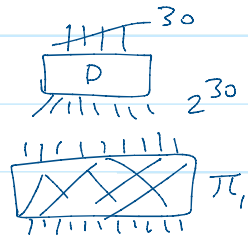
$[\ ,\ ,\ ]$

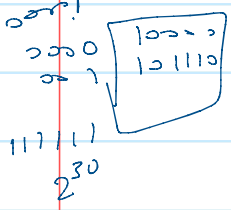
Quiz 2

a. DES. 16

b. Tripple DES. $3 \times 16 = 48$

c. AES 192-bit key. 12



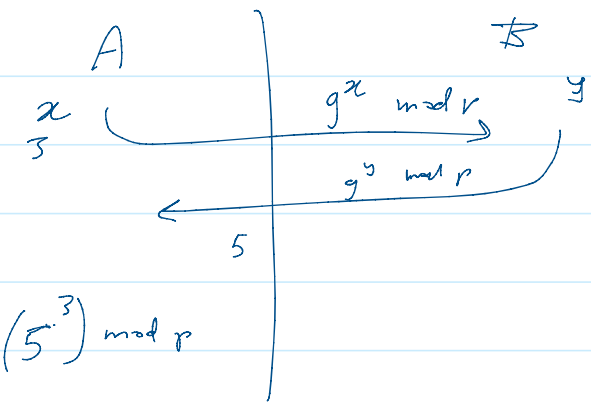


2. [2 pts] Find the key-space in a 30-bit ideal block cipher.

Key size 30×2^{30} ✓ $(2^{30})! = |k|$ ✓

$\pi_{2^{30}!}$

3. [2 pts] Consider Diffie-Hellman key-exchange protocol, with $p = 19$ and $g = 2$. Suppose Alice chose a private-key 3, and she received 5 from Bob. Compute the secret shared key.



Secret Key $(5^3) \bmod p$

(2^3)

$N \cdot n$ $\quad 30 \times 2^{30}$

RSA : $p = 5$, $q = 11$

$n = 5 \times 11 = 55$

$\Phi(n) = 40$

$d = e^{-1} \pmod{40}$

$= 27$

$3 \times 13 \equiv -1$

$3 \times (-13) = -1$

27

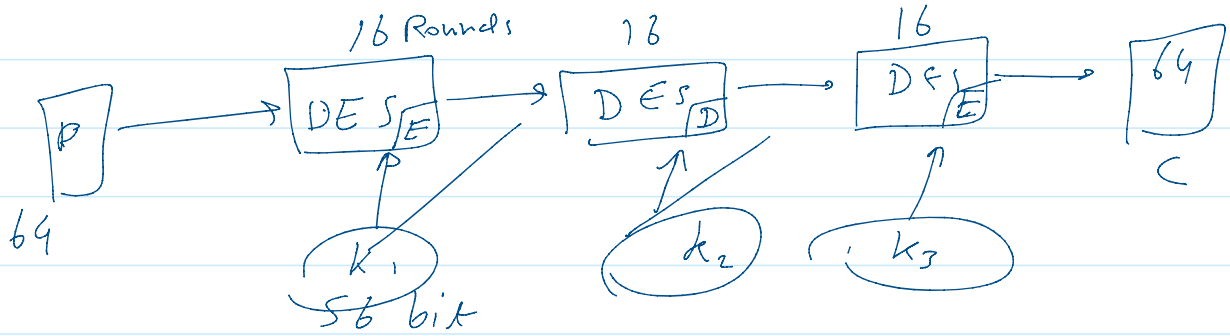
3

$81 \equiv 1 \pmod{40}$

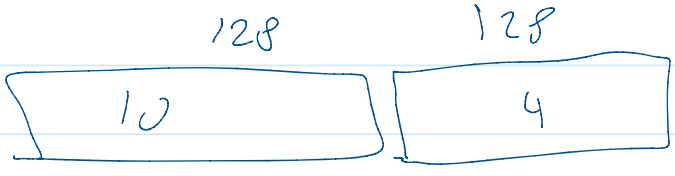
27

$9 \quad 3 \cdot 3$

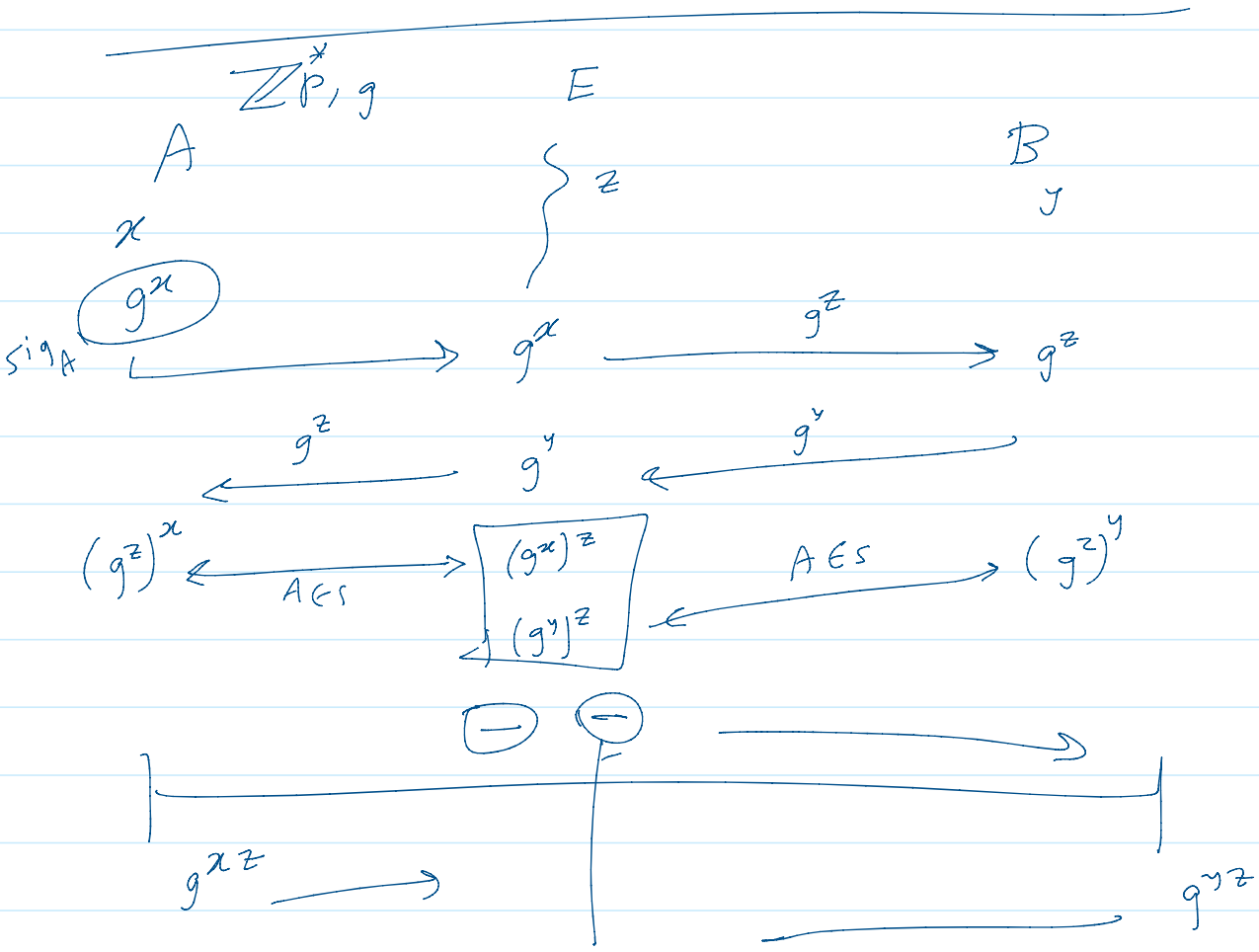
2DES 3DES



"Backword compatibility"



E


$Z_{p,g}^*$
E
A
B
x
y
z
g^x
sig$_A$
g^x
g^z
g^z
g^z
g^y
g^y
$(g^z)^x$
AES
$(g^x)^z$
$(g^y)^z$
AES
$(g^z)^y$
g^{xz}
g^{yz}