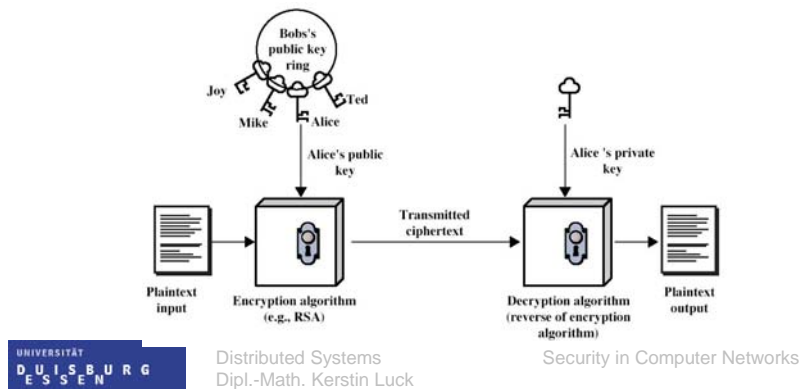




## Asymmetric Ciphers

- New approach: two keys for each party
  - A public key that is available for everybody.
  - A private key that is only available for the owner.



## Asymmetric Ciphers

- Public key encryption or asymmetric ciphers are based on mathematical “trap doors” like the “problem of factorization”.
- This problem is used by the RSA algorithm and means that it's hard to factorize a number which consists of two large prime numbers.
- RSA was published in 1978 by Ronald Rivest, Adi Shamir and Leonard Adleman.

## RSA Key

- The public key is the value pair  $e$  and  $n$ .  
 $KU = \{e, n\}$
- The private key is the value pair  $d$  and  $n$ .  
 $KR = \{d, n\}$

## RSA Key Generation

- Select two large prime numbers  $p$  and  $q$ .
- Calculate  $n = p \cdot q$
- Calculate  $\phi(n) = (p-1)(q-1)$
- $e$  can be chosen free, but must hold the following conditions:  
$$\gcd(\phi(n), e) = 1 \quad \text{and} \quad 1 < e < \phi(n)$$
- Then,  $d$  is computed as the multiplicative inverse of  $e$  mod  $\phi(n)$ .  
$$d \cdot e \bmod \phi(n) \equiv 1 \quad \Rightarrow \quad d \equiv e^{-1} \bmod \phi(n)$$

## RSA Encryption and Decryption

- Encryption:

$$C \equiv M^e \pmod{n}$$

- Decryption:

$$M \equiv C^d \pmod{n}$$

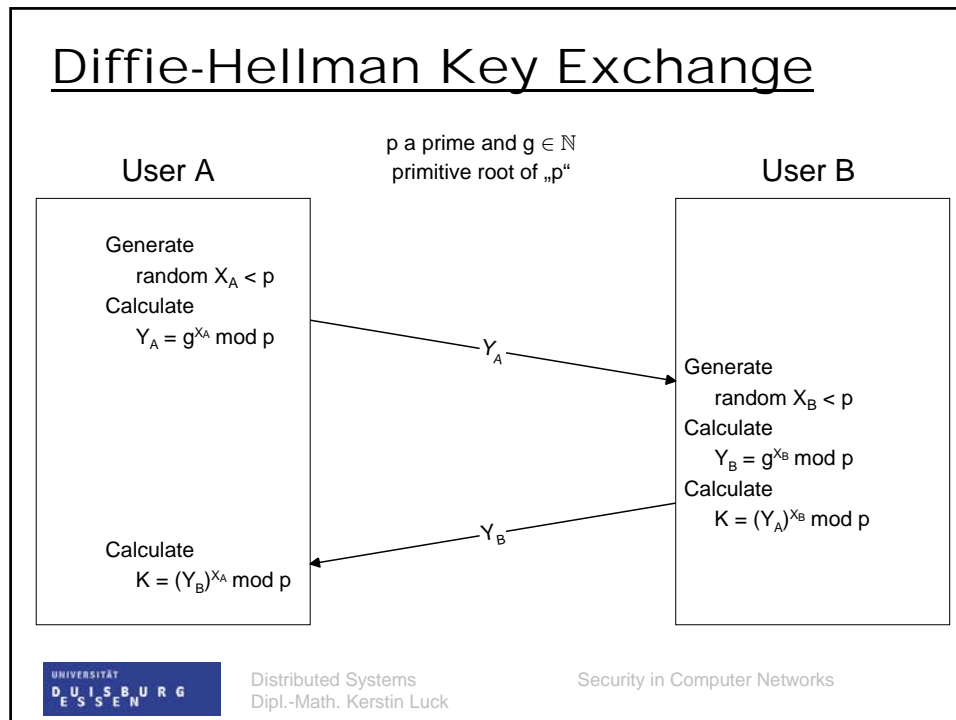
$$\equiv (M^e)^d \pmod{n}$$

$$\equiv M^{e \cdot d} \pmod{n} = M \quad (\text{for } M < n)$$

## Key Exchange

- Another approach is the online key exchange.
- The very first key exchange algorithm was presented by Whitfield Diffie and Martin Hellman, the *Diffie-Hellman Key Exchange*.
- Session keys are generated by private and public information.

## Diffie-Hellman Key Exchange



## Equality of both Results

$$\begin{aligned} K \text{ (of User A)} &\equiv (Y_B)^{X_A} \bmod p \\ &\equiv (g^{X_B} \bmod p)^{X_A} \bmod p \\ &\equiv (g^{X_B})^{X_A} \bmod p \\ &\equiv (g^{X_A})^{X_B} \bmod p \\ &\equiv (g^{X_A} \bmod p)^{X_B} \bmod p \\ &\equiv (Y_A)^{X_B} \bmod p \\ &\equiv K \text{ (of User B)} \quad \textit{q.e.d.} \end{aligned}$$

# Security in Computer Networks

