Special Topics in Cryptography

Mohammad Mahmoody

Last time

- How to combine CPA security + MACS:
- Security against active attacks
- CCA secure private-key encryption

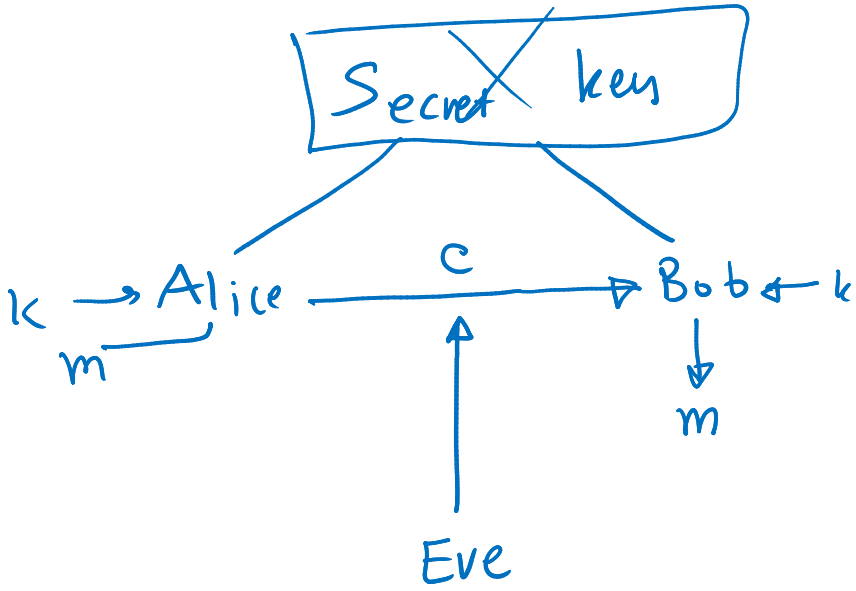
Today

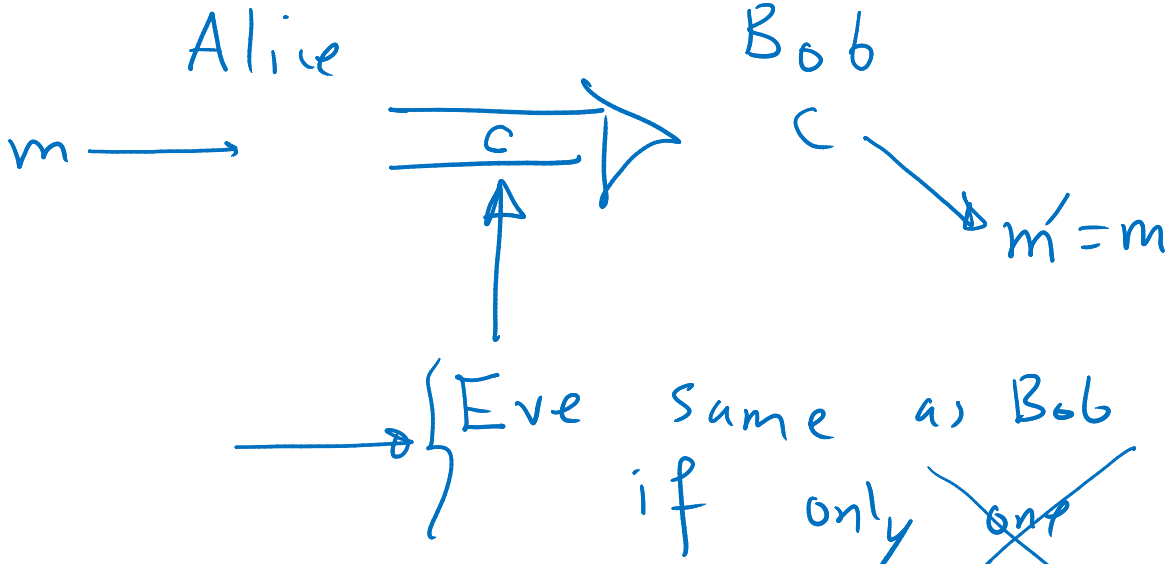
- Public-key encryption and key-agreement
- RSA (PKE) and Diffie Hellman (KA)

Public Key Encryption

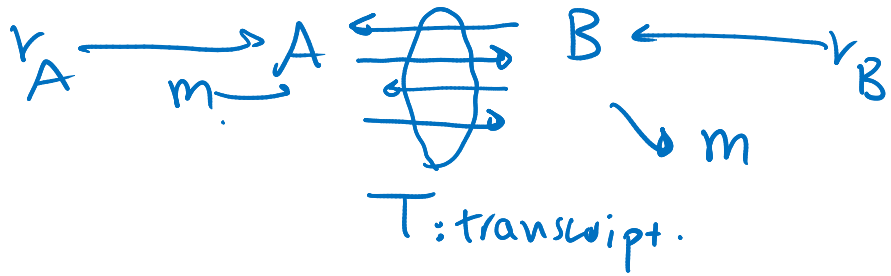
- Secure communication even without shared secret keys!

Main challenge: starting from **zero**



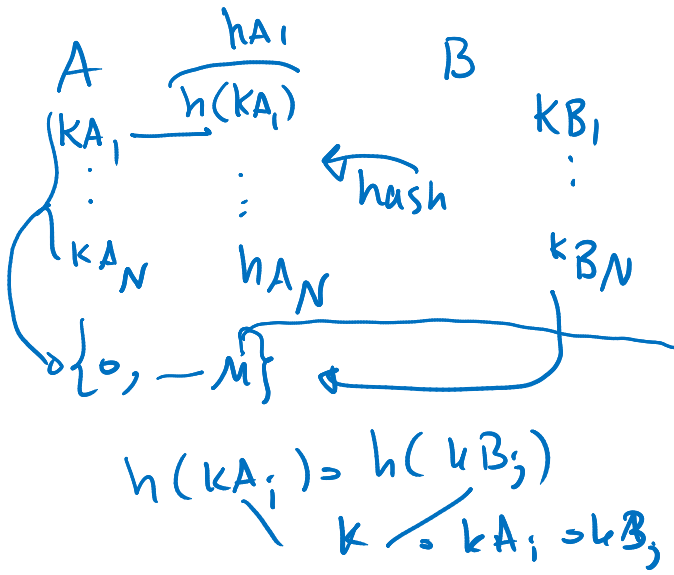


Hope: We can communicate m "interactively"



Intuitive:

http://www.merkle.com/1974/



Project 2 looks more reasonable, maybe because your description Project 1 is muddled terribly. Talk to me about these today.

Ralph Merkle

C.S. 244
FALL 1974

Project Proposal

Topic: Establishing secure communications between seperate secure sites over insecure communication lines.

Assumptions: No prior arrangements have been made between the two sites, and it is assumed that any information known at either site is known to the enemy. The sites, however, are now secure, and any new information will not be divulged.

Method 1: Guessing. Both sites guess at keywords. These guesses are one-way encrypted, and transmitted to the other site. If both sites should chance to guess at the same keyword, this fact will be discovered when the encrypted versions are compared, and this keyword will then be used to establish a communications link.

Discussion: No, I am not joking. If the keyword space is of size N, then the probability that both sites will guess at a common keyword rapidly approaches one after the number of guesses exceeds sqrt(N). Anyone listening in on the line must examine all N possibilities. In more concrete

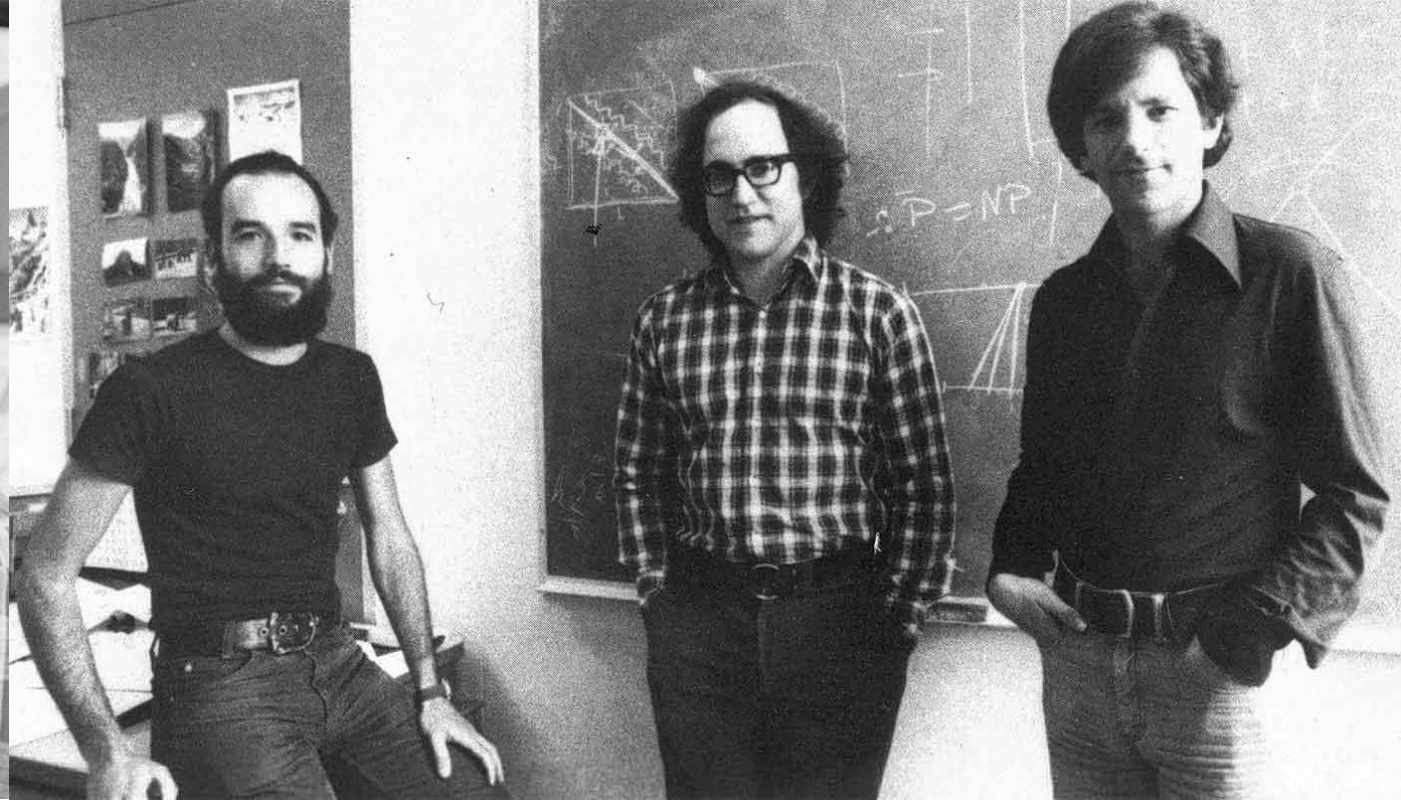
Dear Ralph:

Enclosed is a referee report by an experienced cryptography expert on your manuscript "Secure Communications over Insecure Channels." On the basis of this report I am unable to publish the manuscript in its present form in the Communications of the ACM.

I also read the paper myself and was particularly bothered by the fact that there are no references to the literature. Has anyone else ever investigated this approach. If they consider it and reject it, why? Also, have you considered the fact that E may be willing to devote substantial resources to breaking the code? What makes you think an N^2 amount of effort is a deterrent, particularly since your solution allows E to set N code-breakers to work in parallel, each requiring N units to solve one of the puzzles?

I hope these comments and those of the referee will be of help to you in future work on the subject.

Thank you for submitting your manuscript for publication. Your interest is greatly appreciated.



Merkle

Hellman Diffie

Shamir

Rivest

Adleman

74

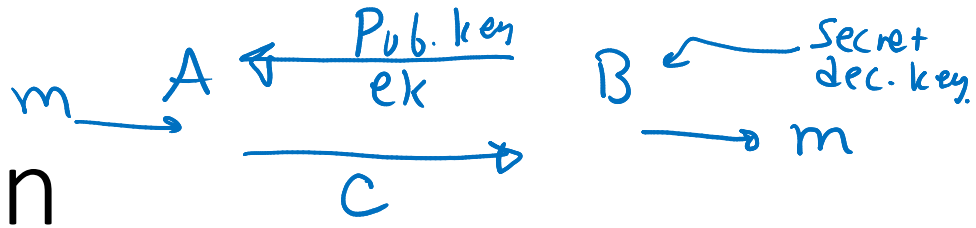
75 x rej

76

78

RSA

Defining Public Key Encryption



Private key

key

$Gen(1^n) \to k \quad |k| = n$

randomized

Public

$Gen(1^n) \to (ek, dk)$

Secret

$Enc(k, m, r) \to c$

ek

$Enc(ek, m, r) \to c$

$Dec(k, c, r') \to m'$

dk

$Dec(dk, c, r') = m'$

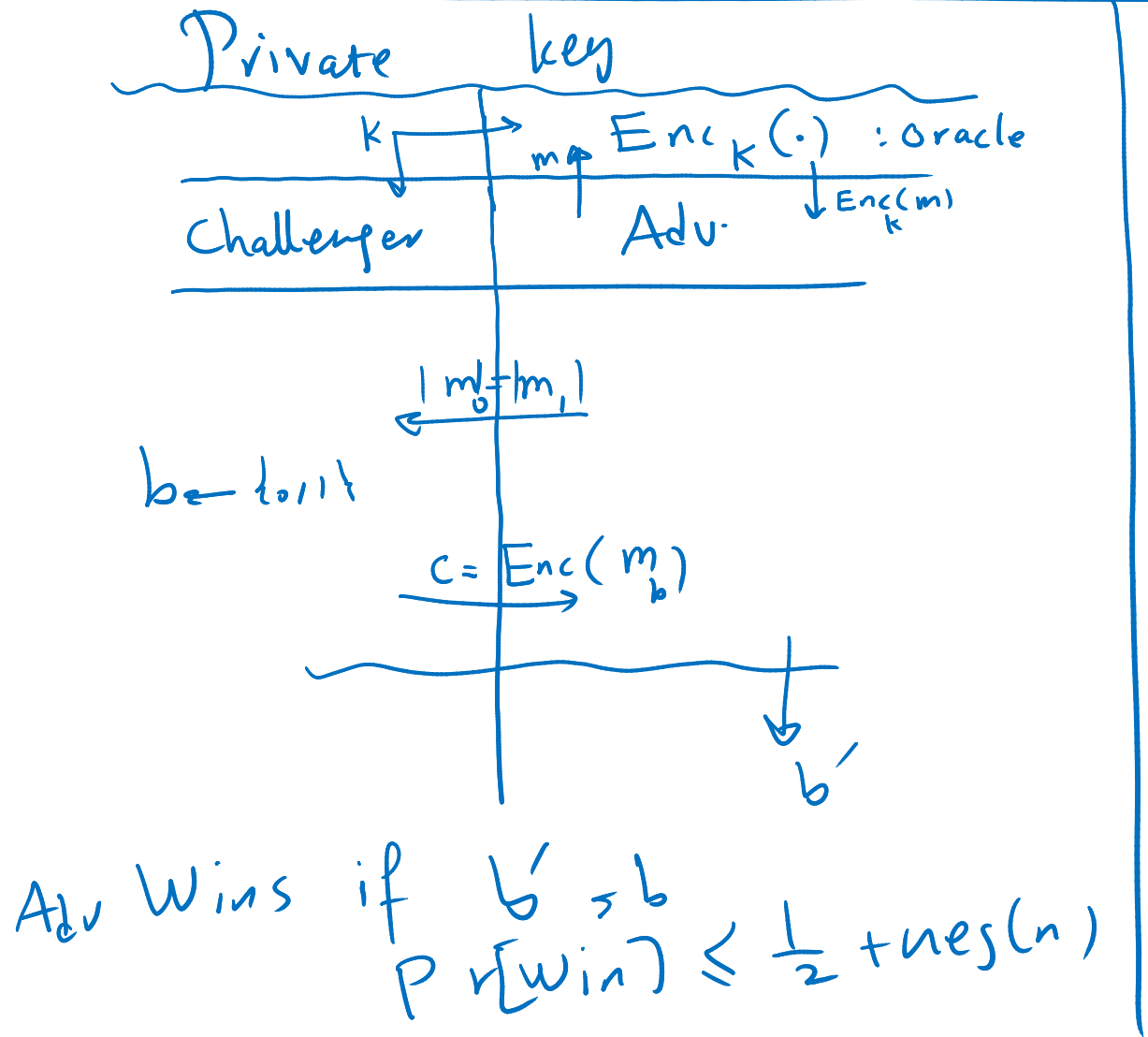
$\forall k, m, r, r' : m' = m$

$\forall (ek, dk) \leftarrow Gen(1^n)$
$m, r, r' :$

$m = m'$

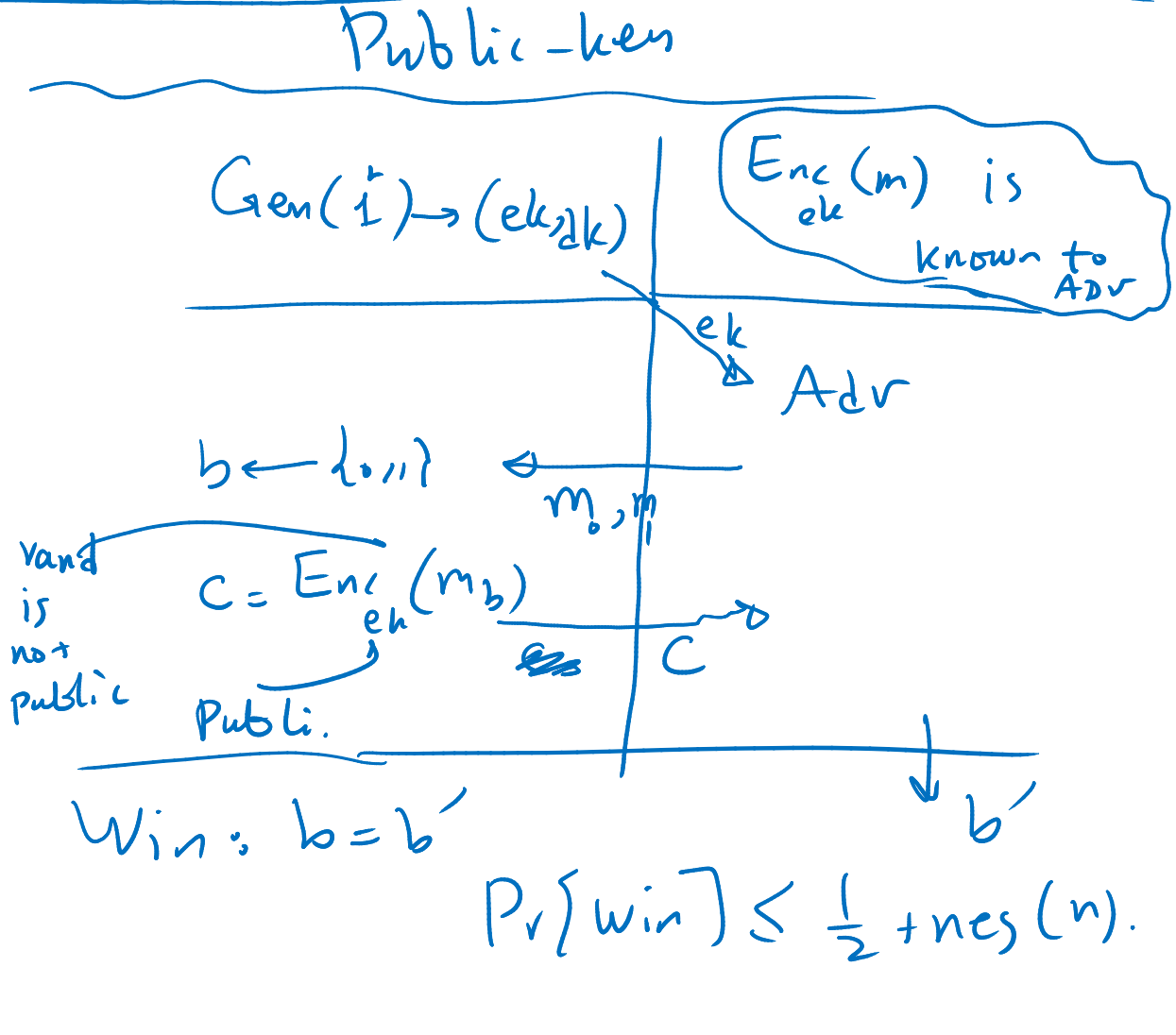
$Gen(1^n) \longrightarrow (ek, dk)$

Security of Public Key Encryption



Adv Wins if $b' = b$

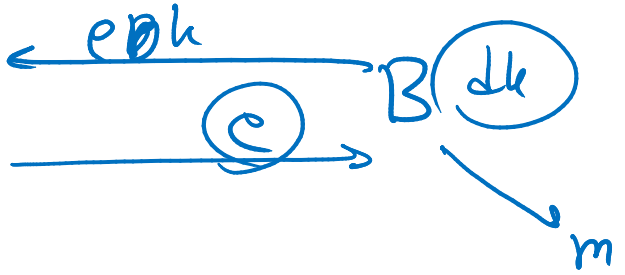
$Pr[Win] \leq \frac{1}{2} + negl(n)$

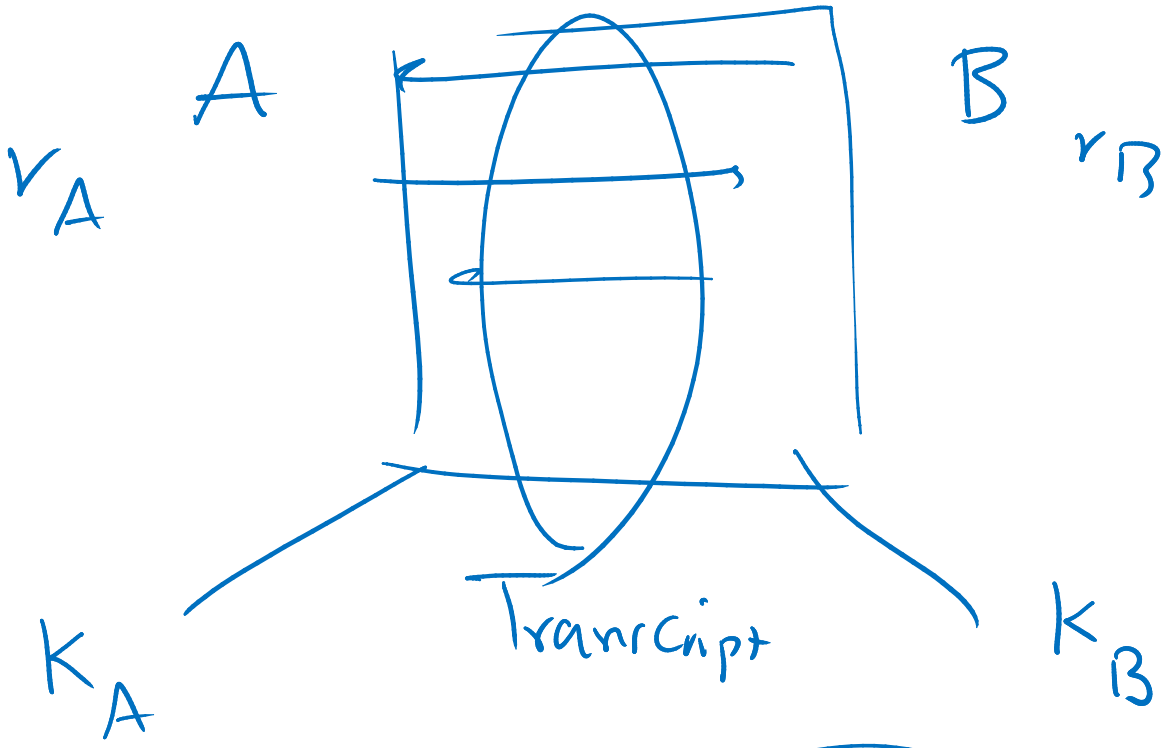


Win: $b = b'$

$Pr[win] \leq \frac{1}{2} + negl(n)$.

A related problem: key agreement



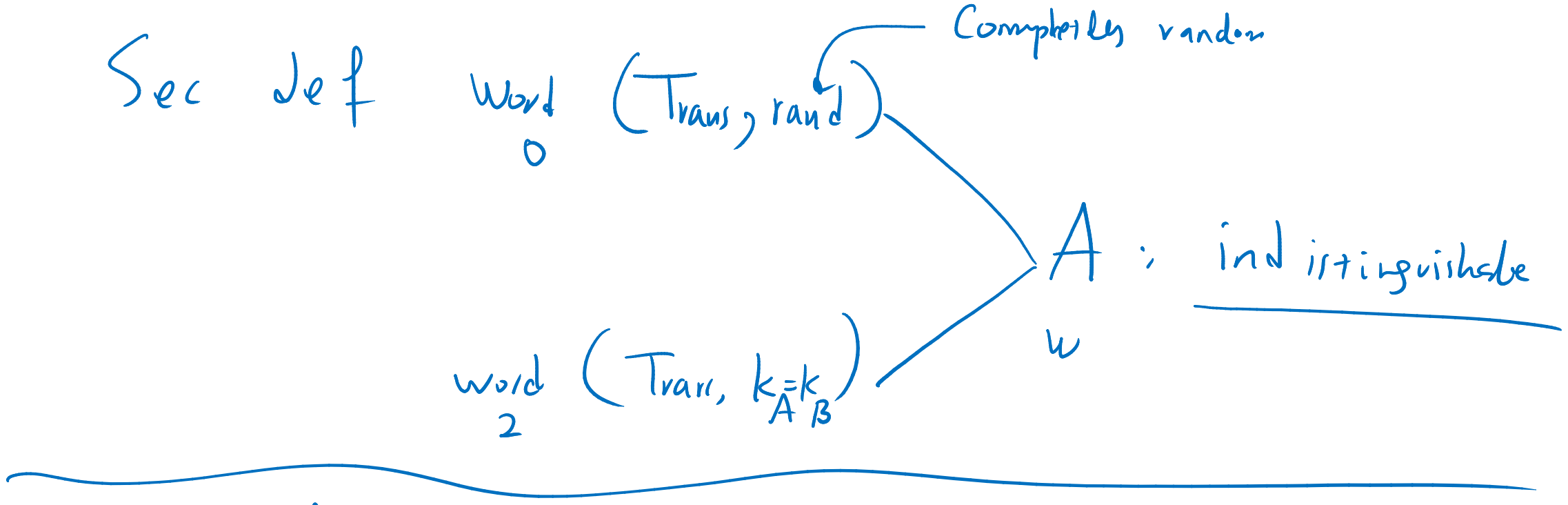


Sec?
Goal: if we use k to enc/dec using private-key schem:
$C = Enc(m,k,r)$
from A to Bob...

Completeness $K_A = K_B = k$ with prob 1

it remain "secure"

Security of Key Agreement



Thm: if we use secure KA + CPA-secure-Secret key Enc.

⟶ ADV who knows Trans + Ciphertext

Number Theory 101: Modular Computation

- $\mathbb{Z}$: integers, can be added (+), subtracted (−) and multiplied (∗)
- Z_N : integers "mod N" : again we can do + , − , ∗
- Interesting cases for us:
  $N = q$ for prime q
  $N = p.q$ for primes p, q
- g is a (multiplicative) generator if: $\{g^0, g^1, \ldots, g^{N-1}\} = \{1, 2, \ldots N-1\}$

Diffie Hellman Key Agreement

Security of Diffie Hellman: Hardness of Discrete Logarithm …

If Discrete Log problem is solvable in polynomial time ⟶ we can break Diffie Hellman.