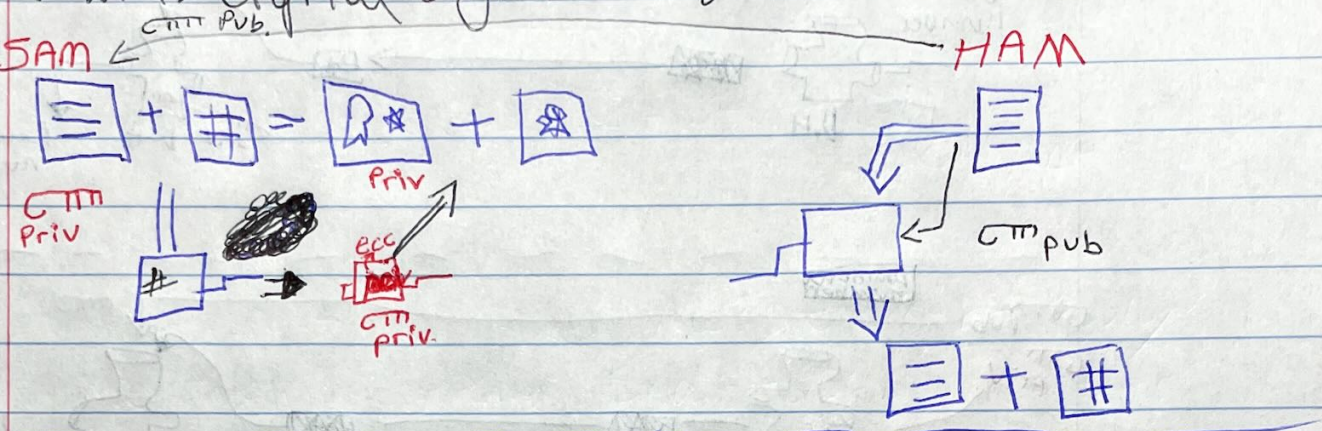
William Prado
07/07/2025

sunny classroom

ITB 1- What is digital signature?

07/07/25



Symetric

Single key

"secret"

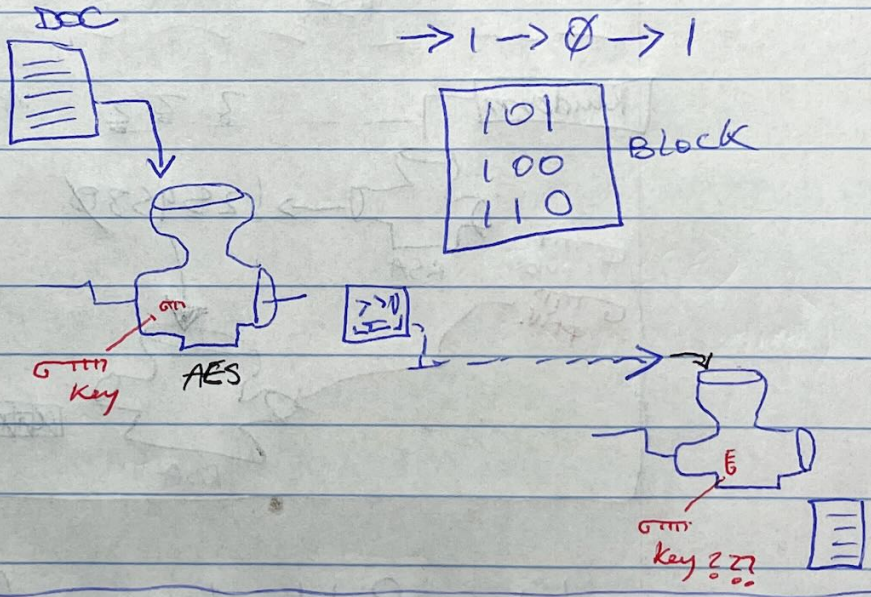
BC4; AES, DES

Fishes

"confidentiality"

What is the issue?

"Bulk encryption"



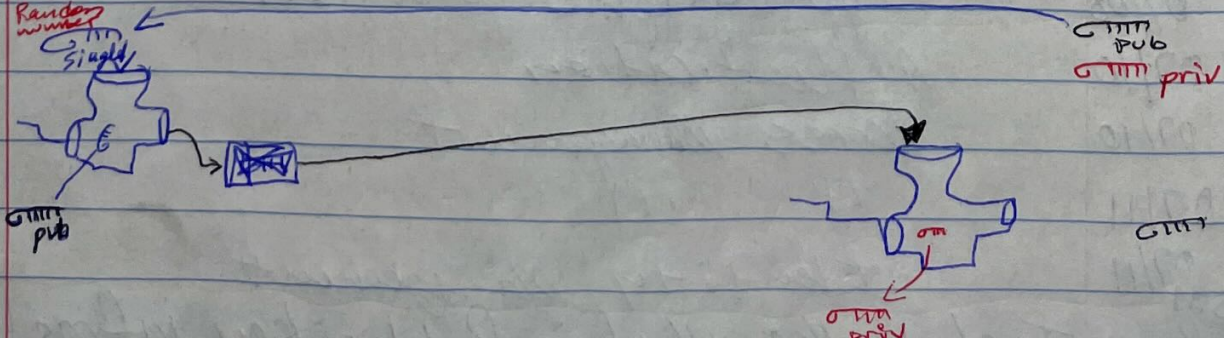
Asymmetric

2Keys

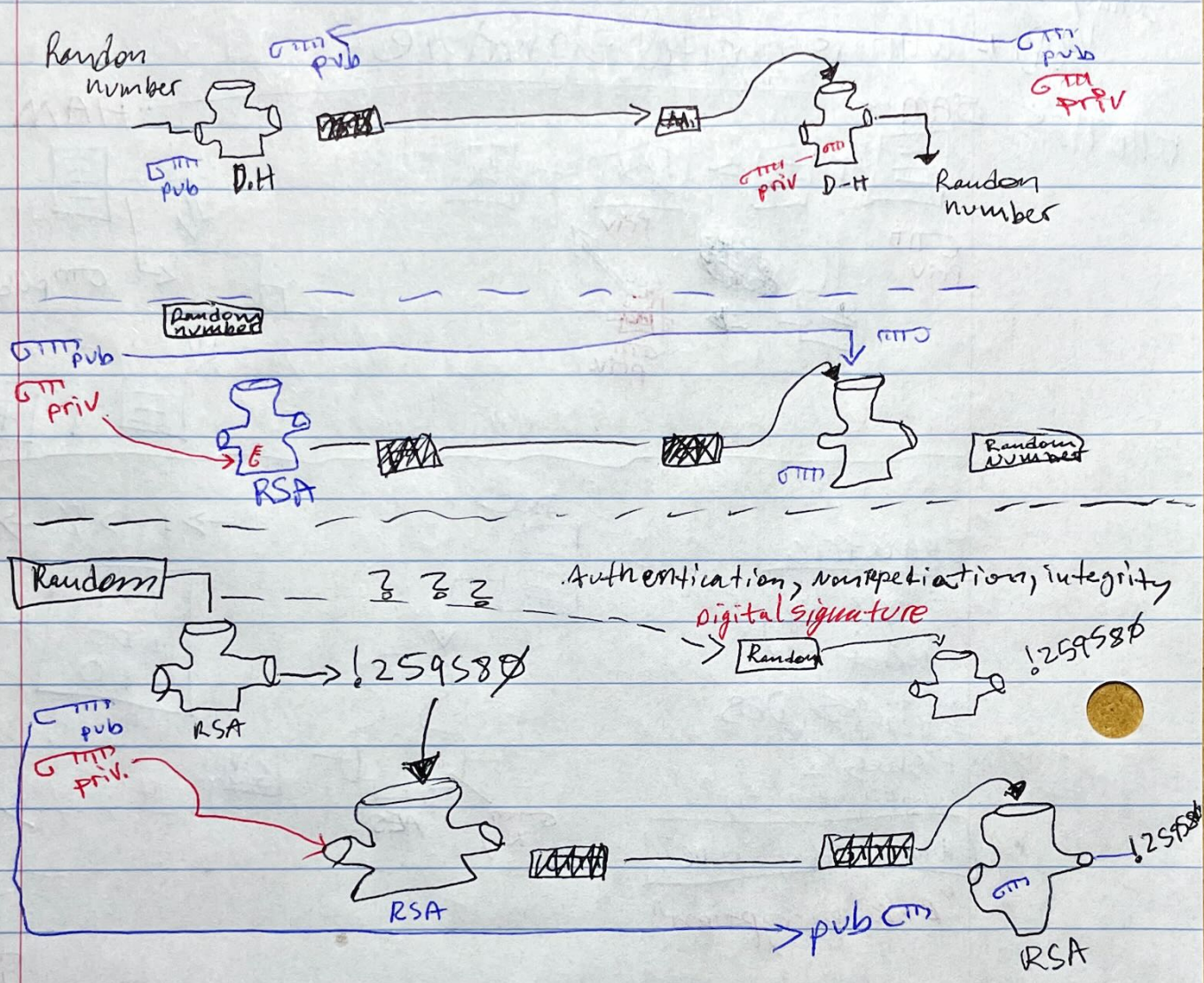
pub
priv

D-H, BSA/DSA, ECC

ECDSA.



William Prado
07/07/2025



YTB ⇒ What is Public key infrastructure? PKI

self signed certificate - do it on your own certificate.

07/07	3B	Public key Infrastructure
07/08		Cryptographic solution
07/10		Authentication
07/10		Access Management
07/11		" "
07/11		Identity Management

IBM
YTB → Tech talk: What is Public key infrastructure (PKI)?

William Prado
07/07/2025

Sunny Classroom
YTB → Why digital certificate?

"Certificate Request"
CR
 questions about you!
Who you are?
Blah, Blah, Blah

Sunny Classroom
YTB → PKI - trust & chain of trust - why, who & how?

Chain of trust - certificate,

Sunny Classroom
YTB Revocation of digital certificates: CRL, OCSP, OCSP stapling

CRL = Certificate Revocation List
OCSP = Online Certificate Status Protocol
CR = Certificate Repository
RA = Registration Authority

Sunny Classroom
YTB Self signed SSL certificate

tomorrow: Private key into a chip.