**BST wyklad 6 – 5.04.2022**

Insfrastruktura klucza publicznego nie zapewnia zaufania do klucza publicznego ani do jednostki

HASHE

Integralnosc danych – wryfikacja za pomocą skrotu wiadomości (hash=skrot),

Skrot wiadomości to wynik działania funkcji hashujacej,

Wazne żeby trudno było wrocic do danych (wiadomości)

Funkcja hash – funkcja jednokierunkowa,

Odpornosc na kolizje – czy podpisując skrot podpisujemy wlasciwy caly dokument,

Dobre funkcje hashujace powinny być odporne na kolizje

Kolizja – dwa rozne dokumenty o takim samym skrocie po funkcji hashujacej (ten sam hash roznych dokumentów) – ŹLE

Łatwiej znaleźć dwa rozne dokumenty żeby miały ten sam skrot, niż do odpowiedniego dokumentu z z określonym skrotem dobrac taki drugi żeby dal ten sam skrot.

Wielkosc danych, dokumentu nie ogranicza nas do zastosowania funkcji skrotu,

Skrot powinien silnie zalezec od każdego bitu dokumentu ( duza lawinowosc)

Skrot powinien być liczony bardzo szybko – duza wydajnosc

Kolizje cos ważnego!! – chociażby z punktu widzenia generowanych podpisow elektronicznych

Skrot bezpieczny ile bitow powinien mieć by nie powodować kolizji?? – obecnie nie mniej niż 224 bity

Funkcje skrotu – z klczem i bez klucza – z kluczem daja możliwość uwierzytelniania

SHA-2 – secure hash algorithm – standard

Dokument dzielimy na bloki dl 1024 bity, na początku wektor inicjalizacji podajemy, dane bloku podajemy działaniu pewnej funkcji F i ixorujemy z wektorem inicjalizacyjnym i podajemy na wyjście – wejście kolejnego bloku – (jako kolejny wektor inicjalizacji)

Za chwile SHA-3 wyprze SHA-2, SHA3 – przyszlosc proszę państwa