Times New Roman Arial Courier New [BoldFont =simhei.ttf, ItalicFont =simkai.ttf|simsun.ttf AR PL UMing CN AR PL UMing CN



éńŸæĂĺ

çaŢåŊŽè£đèŕż,

æIJňçğŚ,

äÿłäžžä£aæAŕ

åĞžçŤ§æŮěæIJ§1989åźť2æIJĹ5æŮě

çğżåŁĺçŤţèŕl 18810459901

Email gaosi11@mails.ucas.ac.cn

éĂŽèőŕålJřålĂ åŇŮäžňåÿĆæţůæůĂåŇžäÿŋåĚşælŚåŊŮåŻŻèąŮ4åŔů

äÿŋåŻ¡çğŚåŋęéŹćè¡ŕäżűçăŤçľűæĽÅ5åŔůæěij

æŢŹèĆšèČŇæŹŕ

2011-èĞşäżŁ èőąçőŮælJžåžŤçŤĺæŁĂælJŕ,

äÿŋåŻ¡çğŚåŋęéŹćè¡ŕäżűçăŤçľűæĽĂ. çăŤçľűæŰźåŘŚïijŽåŔŕä£ąèőąçőŮäÿŐä£ąæĄŕä£léŽIJ

åŕijåÿĹ: åŘťæŰĞçŐš çăŤçľűåŚŸ

åŋęa¡ĎeőžæŰĞécŸçŻő: âÁIJçĄrċZŠæĺąåđŃâĂlaÿŃçŽĎåŕĘçăĄæĺąålŮåőđçŐråőĽåĚĺæĂğåĹĘæđŘ

2007-2011 èőąçőŮælJžçğŚåŋęæŁĂælJŕ,

æŋęæśĽåďǧåŋęèőąçőŮæIJžåŋęéŹć.

äÿŞäÿŽ: ä£ąæĄŕåőĽåĚĺ GPA æŐŠåŘN– 1/90

çăŤçľűéąźçŻő

äÿŋåŻ¡çğŚåŋęéŹćè¡ŕäżűçăŤçľűæĽĂ

2015-èĞşäżŁ å§žäžŐælJžåŹĺåŋęäźăæŁĂælJŕçŽĎä; ğä£ąéĄŞåĹĘæđŘæŰźæşŢ.

- o åĹľçŤĺæŢřåŋŮçďžæşćåŹĺèĞłåŁĺåŇŰéĞĞéŻĘæţŃéĞŔåŕĘçăĄèő¿åďĞè£ŘèąŇæŮűäžğç®
- o åĹľçŤĺäÿżæĹŘåĹĘåĹĘæđŘãĂĄçž£æĂğåĹďåĘşåĹĘæđŘçŋĽæŁĂæIJŕåŕźæĽĂå¿ŮçŽĎèČjéĞŔ
- o æŔŘåĞžåĹľçŤĺçŃňçńŃåĹĘéĞŔåĹĘæđŘæŁĂæIJŕåĹĘæđŘèČjéĞŔæşĎéIJšïijŇæĄćåďŊcŤţèůi

2013-2015 å§žäžŐä¿ğä£ąéĄŞåĹĘæđŘçŽĎéĂĘåŘŚåĹĘæđŘ.

- o åĹĺçŤĺeČjeGRæşDeIJsä£ąæĄriijNaĹĘæďŘánęažáeő¿áďĞçŽĎåődçŐřæŰźåijŔ
- éĂŽè£Ğ瞣æĂğåŻđ塊åĹĘæđŘæĄćåďŊèő¿åďĞäÿŋä¡£çŤĺçŽĎåŕĘçăĄçőŮæşŢ

2012-2014 äÿħåŘŇåőđçŐřæŰźåijŔåŕźäžŐåŕĘçăĄçőŮæşŢåőĽåĚĺæĂğå¡śåŞħçŽĎåĹĘæđŘäÿŐ

- o äÿzèęĄåĚşæşĺ PKCS#1 v1.5 (çŻőåĽŊæIJĂåź£æşŻä¡£çŤĺçŽĎäÿŁäÿĂäżčRSAåŁăåŕĘæăĞåĞ
- éAnaŐĘäžĘaŘĎçğnaŔŕeČjçŽĎaődçŐřæŰźaijŔiijŇaŕźažŐæŕŔçğnaődçŐřæŰźaijŔaĹĘaĹńçz

äÿŞäÿŽæŁĂèČ¡

èrηèÍ \check{A} äÿηæ $\check{U}\check{G}$ / è \check{N} sèrη (CET-6)

çĺŃåžŔèŕŋèĺĂ C, C#, Java, Verilog.

åijĂåŔŚåůěåĚů Microsoft Visual Studio, NetBeans IDE, Modelsim, Design Compiler

åŔĆäÿŐçńđèţŻ, äÿŞåž獺èŕů & èőžæŰĞåŔŚèąĺ åŔĆäÿŐçńđèţŻ

- 2010 åĔĺåŻ¡ådgåŋę獧çŤţåŋŘèő¿èőąçńđèţŻ(ä£ąæĄŕåőĽåĔĺéĆĂèŕůèţŻ), äÿĽçŋĽåěŰ.
- 2010 åĚĺåŻ¡åďgåŋę獧ä£ąæĄŕåőĽåĚĺçńđèţŻ, äžŇçŋĽåěŰ.

äÿŞåž獺èŕů

2013 âĂIJäÿĂçğDåŕĘçăĄæĺąåİŮAPIåőĽåĚĺæĂğæčĂæţŃæŰźæşŢåŔŁçşżçż§âĂİ (äÿŞåĹľåŔůïijŽZL 201310013010.4)

èőžæŰĞåŔŚèaĺ

- 2013 "Padding Oracle Attack on PKCS#1 v1.5: Can Non-standard Implementation Act as a Shelter?", Cryptology and Network Security 2013.
- åuså¡ŢçŤĺ "Improved fault attack on LBlock: earlier injection with no extra faults", Chinese Journal of Electronics.

åŘĹä¡IJèőžæŰĞ äÿďçŕĞ: WISA 2013/SAC 2015