Suggested Topics for Student Presentations

Expectations brief notes, "newspaper headline grammar"

- Clearly state attacking scenario
    - Ex: If small private exponent attack → how small is d? If partial key exposure attack → does the attacker know some MSBs of d? LSBs? Or bits in any position? If attack on RSA variant → how is the variant defined?
- Point out connections to materials covered in my lectures (if applicable)
    - Ex: If Coppersmith's method → briefly review lattice method in RSA cryptanalysis
- Clearly state preliminaries
    - Ex: If extension of Wiener's attack → say what conclusions about continued fractions will be used in attack (you don't need to show the proofs of theorems in preliminaries)
- Explain how attack goes, and why it works (main part)
    - If simple attack, describe it in full
    - If not, at least describe it in sufficient detail so that people can have a clear idea on how it works; also clearly explain what's missing
    - If reasoning simple, give full proof
    - If not, at least explain it in sufficient detail so that people can be reasonably convinced that it works

Logistics

Current plan:

Weeks 4-6 (10/20-11/05): I talk about algorithms for discrete logarithm and its variants

Week 7: No classes, prepare your presentations

Weeks 8-10 (11/17-12/03): Your presentations (cancel 11/26 class before Thanksgiving?)

Topic 1: Coppersmith's method for finding small roots

1.1 Original Coppersmith's method

*[Coppersmith96a] Don Coppersmith. Finding a Small Root of a Univariate Modular Equation. In *EUROCRYPT 1996*.

[AASW12] Yoshinori Aono, Manindra Agrawal, Takakazu Satoh, and Osamu Watanabe. On the Optimality of Lattices for the Coppersmith Technique. In *ACISP 2012*. // Coppersmith's bound is optimal when applying the LLL algorithm to RSA cryptanalysis

1.2 Extensions of Coppersmith's method

*[Coppersmith96b] Don Coppersmith. Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In *EUROCRYPT 1996*. // two contributions: (1) extending Coppersmith's method to the bivariate equation case; (2) factor N when you have a (somewhat accurate) estimation of p or q

[Jutla98] Charanjit S. Jutla. On Finding Small Solutions of Modular Multivariate Polynomial Equations. In *EUROCRYPT 1998*.

[Coron04] Jean-Sébastien Coron. Finding Small Roots of Bivariate Integer Polynomial Equations Revisited. In *EUROCRYPT 2004*.

[BM05] Johannes Blömer and Alexander May. A Tool Kit for Finding Small Roots of Bivariate Polynomials over the Integers. In *EUROCRYPT 2005*.

[JM06] Ellen Jochemsz and Alexander May. A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants. In *ASIACRYPT 2006*.

[BJ07] Aurélie Bauer and Antoine Joux. Toward a Rigorous Variation of Coppersmith's Algorithm on Three Variables. In *EUROCRYPT 2007*.

[Coron07] Jean-Sébastien Coron. Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach. In *CRYPTO 2007*.

[Aono13] Yoshinori Aono. Minkowski Sum Based Lattice Construction for Multivariate Simultaneous Coppersmith's Technique and Applications to RSA. In *ACISP 2013*.

[FLCNP25] Yansong Feng, Hengyi Luo, Qiyuan Chen, Abderrahmane Nitaj, and Yanbin Pan. Computing Asymptotic Bounds for Small Roots in Coppersmith's Method via Sumset Theory. In *CRYPTO 2025*. // computes det(B) more efficiently

Appendix Surveys of Coppersmith's method

// do not present these papers per se; these are second-hand sources that help you understand the original papers better

*[Galbraith18] Steven Galbraith. Coppersmith's Method and Related Applications. https://www.math.auckland.ac.nz/~sgal018/crypto-book/ch19.pdf

*[May21] Alexander May. Lattice-based Integer Factorization – An Introduction to Coppersmith's Method. https://www.cits.ruhr-uni-bochum.de/imperia/md/content/may/paper/intro_to_coppersmiths_method.pdf

Topic 2: More related plaintext attacks

*[MR08] Alexander May and Maike Ritzenhofen. Solving Systems of Modular Equations in One Variable: How Many RSA-Encrypted Messages Does Eve Need to Know? In *PKC 2008*.

Topic 3: More small private exponent attacks

3.1 Limitations of Wiener's attack

*[SCWP05] Ron Steinfeld, Scott Contini, Huaxiong Wang, and Josef Pieprzyk. Converse Results to the Wiener Attack on RSA. In *PKC 2005*.

3.2 Extensions of Wiener's attack

*[VT97] Eric R. Verheul and Henk C. A. van Tilborg. Cryptanalysis of 'Less Short' RSA Secret Exponents. In *Applicable Algebra in Engineering, Communication and Computing 8*.

*[Dujella04] Andrej Dujella. Continued Fractions and RSA with Small Secret Exponent. https://arxiv.org/pdf/cs/0402052

*[SWC07] Hung-Min Sun, Mu-En Wu, and Yao-Hsin Chen. Estimating the Prime-Factors of an RSA Modulus and an Extension of the Wiener Attack. In *ACNS 2007*.

*[Dujella08] Andrej Dujella. A variant of Wiener's attack on RSA. https://eprint.iacr.org/2008/459.pdf

*[Nitaj08] Abderrahmane Nitaj. Another Generalization of Wiener's Attack on RSA. In *AFRICACRYPT 2008*.

*[Nitaj10] A New Vulnerable Class of Exponents in RSA. https://nitaj.users.lmno.cnrs.fr/rsa10.pdf // not actually small private exponent attack; attack similar to Wiener's attack

3.3 Lattice-based small private exponent attacks (combining Wiener's attack and Coppersmith's method)

*[BD99] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with Private Key *d* Less than $N^{0.292}$. In *EUROCRYPT 1999*.

[BM01] Johannes Blömer and Alexander May. Low Secret Exponent RSA Revisited. In *CaLC 2001*.

[BM04] Johannes Blömer and Alexander May. A Generalized Wiener Attack on RSA. In *PKC 2004*.

[MS08] Subhamoy Maitra and Santanu Sarkar. A New Class of Weak Encryption Exponents in RSA. In *INDOCRYPT 2008*.

[HM10] Mathias Herrmann and Alexander May. Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. In *PKC 2010*.

[KSI11] Noboru Kunihiro, Naoyuki Shinohara, and Tetsuya Izu. A Unified Framework for Small Secret Exponent Attack on RSA. In *SAC 2011*. // covers several existing attacks as special cases

[LZQ23] Qiang Li, Qun-xiong Zheng, and Wen-feng Qi. Practical Attacks on Small Private Exponent RSA: New Records and New Insights. In *Designs, Codes and Cryptography 91(12)*.

[ZFNP25] Mengce Zheng, Yansong Feng, Abderrahmane Nitaj, and Yanbin Pan. Improving RSA Cryptanalysis: Combining Continued Fractions and Coppersmith's Techniques. In *ACISP 2025*.

3.4 Cryptanalysis of specific RSA instances

[DN00] Glenn Durfee and Phong Q. Nguyen. Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99. In *ASIACRYPT 2000*. // attack on unbalanced instances

[de Weger02] Benne de Weger. Cryptanalysis of RSA with Small Prime Difference. In *Applicable Algebra in Engineering, Communication and Computing 13*. // attack when p and q are close

[ZQ07] Yao-Dong Zhao and Wen-Feng Qi. Small Private-Exponent Attack on RSA with Primes Sharing Bits. In *ISC 2007*. // attack when p and q share some bits (e.g., LSBs)

[SWSGW08] Hung-Min Sun, Mu-En Wu, Ron Steinfeld, Jian Guo, and Huaxiong Wang. Cryptanalysis of Short Exponent RSA with Primes Sharing Least Significant Bits. In *CANS 2008*.

*[MS08] Subhamoy Maitra and Santanu Sarkar. Revisiting Wiener's Attack – New Weak Keys in RSA. In *ISC 2008*. // attack when p and $2q$ are close

3.5 Cryptanalysis of multiple RSA instances with common modulus

*[HS99] Nicholas Howgrave-Graham and Jean-Pierre Seifert. Extending Wiener's Attack in the Presence of Many Decrypting Exponents. In *CQRE [Secure] 1999*.

*[HL10] M. Jason Hinek and Charles C. Y. Lam. Common Modulus Attacks on Small Private Exponent RSA and Some Fast Variants (in Practice). In *Journal of Mathematical Cryptology 4(1)*.

[TK14] Atsushi Takayasu and Noboru Kunihiro. Cryptanalysis of RSA with Multiple Small Secret Exponents. In *ACISP 2014*.

Topic 4: More partial key exposure attacks

*[BDF98] Dan Boneh, Glenn Durfee, and Yair Frankel. An Attack on RSA Given a Small Fraction of the Private Key Bits. In *ASIACRYPT 1998*. // attack when $e \leq \sqrt{N}$

[SZ01] Ron Steinfeld and Yuliang Zheng. An Advantage of Low-Exponent RSA with Modulus Primes Sharing Least Significant Bits. In *CT-RSA 2001*. // [BDF98] doesn't work that well when p and q share some LSBs N

[BM03] Johannes Blömer and Alexander May. New Partial Key Exposure Attacks on RSA. In *CRYPTO 2003*. // attack when $e > \sqrt{N}$

[EJMdW05] Matthias Ernst, Ellen Jochemsz, Alexander May and Benne de Weger. Partial Key Exposure Attacks on RSA up to Full Size Exponents. In *EUROCRYPT 2005*.

[JdW06] Ellen Jochemsz and Benne de Weger. A Partial Key Exposure Attack on RSA Using a 2-Dimensional Lattice. In *ISC 2006*. // attack when *d* is small

[JL12] Marc Joye and Tancrède Lepoint. Partial Key Exposure on RSA with Private Exponents Larger Than *N*. In *ISPEC 2012*.

[TK14] Atsushi Takayasu and Noboru Kunihiro. Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound. In *SAC 2014*. // attack when *d* is small

[TK17] Atsushi Takayasu and Noboru Kunihiro. A Tool Kit for Partial Key Exposure Attacks on RSA. In *CT-RSA 2017*. // covers several existing attacks as special cases

[STK20] Kaichi Suzuki, Atsushi Takayasu, and Noboru Kunihiro. Extended Partial Key Exposure Attacks on RSA: Improvement up to Full Size Decryption Exponents. In *Theoretical Computer Science 841*. // extends [TK14] to arbitrary *d*

4.1 More partial key exposure attacks with known MSBs

[FNP24] Yansong Feng, Abderrahmane Nitaj, and Yanbin Pan. Small Public Exponent Brings More: Improved Partial Key Exposure Attacks against RSA. In *Communications in Cryptology 1(3)*. // attack when *e* is small

4.2 Partial key exposure attacks with known LSBs

[Aono09] Yoshinori Aono. A New Lattice Construction for Partial Key Exposure Attack for RSA. In *PKC 2009*. // attack when *d* is small

Topic 5: Partially known primes attacks

[HM08] Mathias Herrmann and Alexander May. Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits. In *ASIACRYPT 2008*. // attack when you know some bits of *p* at any position

[MSS10] Subhamoy Maitra, Santanu Sarkar, and Sourav Sen Gupta. Factoring RSA Modulus Using Prime Reconstruction from Random Known Bits. In *AFRICACRYPT 2010*.

5.1 Combination with small private exponent attacks

[NBD08] Dieaa I. Nassr, Hatem M. Bahig, Ashraf Bhery, and Sameh S. Daoud. A New RSA Vulnerability Using Continued Fractions. In *AICCSA 2008*.

[SMS08] Santanu Sarkar, Subhamoy Maitra, and Sumanta Sarkar. RSA Cryptanalysis with Increased Bounds on the Secret Exponent using Less Lattice Dimension. https://eprint.iacr.org/2008/315.pdf // attack when d is small and you know some MSBs of p

[FLNP24] Yansong Feng, Zhen Liu, Abderrahmane Nitaj, and Yanbin Pan. Practical Small Private Exponent Attacks against RSA. https://eprint.iacr.org/2024/1331.pdf // attack when d is small and you know some MSBs of $p+q$

5.2 Combination with partial key exposure attacks

[SM08] Santanu Sarkar and Subhamoy Maitra. Improved Partial Key Exposure Attacks on RSA by Guessing a Few Bits of One of the Prime Factors. In *ISC 2008*. // attack when you know some bits of d and also some MSBs of p

[PHHX15] Liqiang Peng, Lei Hu, Zhangjie Huang, and Jun Xu. Partial Prime Factor Exposure Attacks on RSA and Its Takagi's Variant. In *ISPEC 2015*. // attack when you know some bits of d and also some MSBs or LSBs of q

Topic 6: Cryptanalysis of CRT-RSA

// RSA instance with (private) CRT exponents $d_p = [d \bmod p]-1$, $d_q = [d \bmod q]-1$ instead of d; allows for faster decryption

[MS09] Subhamoy Maitra and Santanu Sarkar. Deterministic Polynomial-Time Equivalence of Computing the CRT-RSA Secret Keys and Factoring. In *WCC 2009*.

6.1 Small CRT exponent attacks

[GHM05] Steven D. Galbraith, Chris Heneghan and James F. McKee. Tunable Balancing of RSA. In *ACISP 2005*. // only works for $N^{1/4} \leq e \leq N^{3/4}$

*[JM07] Ellen Jochemsz and Alexander May. A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$. In *CRYPTO 2007*.

[TLP17] Atsushi Takayasu, Yao Lu, and Liqiang Peng. Small CRT-Exponent RSA Revisited. In *EUROCRYPT 2017*.

6.2 Small CRT exponent attacks on unbalanced instances

[May02] Alexander May. Cryptanalysis of Unbalanced RSA with Small CRT-Exponent. In *CRYPTO 2002*.

[BM06] Daniel Bleichenbacher and Alexander May. New Attacks on RSA with Small Secret CRT-Exponents. In *PKC 2006*.

6.3 Partial key exposure attacks

[SM09] Santanu Sarkar and Subhamoy Maitra. Partial Key Exposure Attack on CRT-RSA. In *ACNS 2009*. // attack when you know some MSBs of d_p and d_q; better attack when you additionally know some MSBs of p and q

*[HS09] Nadia Heninger and Hovav Shacham. Reconstructing RSA Private Keys from Random Key Bits. In *CRYPTO 2009*. // attack when you know some bits of d_p and d_q at any position

[LZL14] Yao Lu, Rui Zhang, and Dongdai Lin. New Partial Key Exposure Attacks on CRT-RSA with Large Public Exponents. In *ACNS 2014*.

[TK15] Atsushi Takayasu and Noboru Kunihiro. Partial Key Exposure Attacks on CRT-RSA: Better Cryptanalysis to Full Size Encryption Exponents. In *ACNS 2015*.

[MNS21] Alexander May, Julian Nowakowski, and Santanu Sarkar. Partial Key Exposure Attack on Short Secret Exponent CRT-RSA. In *ASIACRYPT 2021*. // attack when d is small and you know some MSBs or LSBs of d_p and d_q

[MNS22] Alexander May, Julian Nowakowski, and Santanu Sarkar. Approximate Divisor Multiples — Factoring with Only a Third of the Secret CRT-Exponents. In *EUROCRYPT 2022*. // attack when e is small and you know some bits of d_p and d_q at any position

Topic 7: Cryptanalysis of multi-power RSA (a.k.a. Takagi's scheme)

// extension of RSA with $N = p^r q$

// there is another (less-studied) extension with $N = p^r q^s$ (not included below)

[BDH99] Dan Boneh, Glenn Durfee, and Nick Howgrave-Graham. Factoring $N = p^r q$ for Large r. In *CRYPTO 1999*.

[KK07] Noboru Kunihiro and Kaoru Kurosawa. Deterministic Polynomial Time Equivalence Between Factoring and Key-Recovery Attack on Takagi's RSA. In *PKC 2007*.

*[NR15] Abderrahmane Nitaj and Tajjeeddine Rachidi. New Attacks on RSA with Moduli $N = p^r q$. In *C2SI 2015*.

[TK16] Atsushi Takayasu and Noboru Kunihiro. How to Generalize RSA Cryptanalyses. In *PKC 2016*. // generalizes attacks on RSA to attacks on multi-power RSA

7.1 Small private exponent attacks

[May04] Alexander May. Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$. In *PKC 2004*.

[IKK08] Kouichi Itoh, Noboru Kunihiro, and Kaoru Kurosawa. Small Secret Key Attack on a Variant of RSA (Due to Takagi). In *CT-RSA 2008*.

[Sarkar14] Santanu Sarkar. Small Secret Exponent Attack on RSA Variant with Modulus $N = p^r q$. In *Designs, Codes and Cryptography 73(2)*. // better attack when $r \leq 5$

[Sarkar15] Santanu Sarkar. Revisiting Prime Power RSA. In *Discrete Applied Mathematics 203*. // better attack when $r \leq 8$

7.2 Partial key exposure attacks

[LZL13] Yao Lu, Rui Zhang, and Dongdai Lin. Factoring Multi-power RSA Modulus $N = p^r q$ with Partial Known Bits. In *ACISP 2013*.

[HHXPX14] Zhangjie Huang, Lei Hu, Jun Xu, Liqiang Peng, and Yonghong Xie. Partial Key Exposure Attacks on Takagi's Variant of RSA. In *ACNS 2014*.

[EKU15] Muhammed F. Esgin, Mehmet S. Kiraz, and Osmanbey Uzunkol. A New Partial Key Exposure Attack on Multi-power RSA. In *CAI 2015*. // known LSBs

Appendix: PhD theses on RSA cryptanalysis

[Durfee02] Glenn Durfee. Cryptanalysis of RSA Using Algebraic and Lattice Methods. https://theory.stanford.edu/~gdurf/durfee-thesis-phd.pdf

[May03] Alexander May. New RSA Vulnerabilities Using Lattice Reduction Methods. https://d-nb.info/972386416/34

[Jochemsz07] Ellen Jochemsz. Cryptanalysis of RSA Variants Using Small Roots of Polynomials. https://pure.tue.nl/ws/portalfiles/portal/1796260/200711750.pdf

[Hinek07] On the Security of Some Variants of RSA. https://dspacemainprd01.lib.uwaterloo.ca/server/api/core/bitstreams/c1baec8e-ba2e-49ab-8439-11a60b3957fa/content

Topic 8: Discrete logarithm over a sparse set

*[Schnorr01] Claus Peter Schnorr. Small generic hardcore subsets for the discrete logarithm: Short secret DL-keys. In *Information Processing Letters 79(2)*. // contains both an algorithm and lower bounds; only the former is relevant

Topic 9: Variants of Pollard's algorithms

[vOW99] Paul C. van Oorschot and Michael J. Wiener. Parallel Collision Search with Cryptanalytic Applications. In *Journal of Cryptology 12(1)*. // parallel speedup for both rho and kangaroo

9.1 Variants of Pollard's rho

[Teske98] Edlyn Teske. Speeding up Pollard's Rho Method for Computing Discrete Logarithms. In *ANTS 1998*.

[Nivasch04] Gabriel Nivasch. Cycle Detection Using a Stack. In *Information Processing Letters 90(3)*.

[CHK08] Jung Hee Cheon, Jin Hong, and Minkyu Kim. Speeding Up the Pollard Rho Method on Prime Fields. In *ASIACRYPT 2008*. // Pollard's rho in Z_p^*

9.2 Variants of Pollard's kangaroo

[Teske03] Edlyn Teske. Computing Discrete Logarithms with the Parallelized Kangaroo Method. In *Discrete Applied Mathematics 130(1)*.

[GR10] Steven D. Galbraith and Raminder S. Ruprai. Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval. In *PKC 2010*.

[GPR13] Steven D. Galbraith, John M. Pollard and Raminder S. Ruprai. Computing Discrete Logarithms in an Interval. In *Mathematics of Computation 82(282)*. // both 3-kangaroo algorithm (discussed in class) and 4-kangaroo algorithm

[Fowler14] Alex Fowler. Kangaroo Methods for Solving the Interval Discrete Logarithm Problem. https://www.math.auckland.ac.nz/~sgal018/AFhons.pdf // 5-kangaroo algorithm

[ZZYLL19] Yuqing Zhu, Jincheng Zhuang, Hairong Yi, Chang Lv, and Dongdai Lin. A Variant of the Galbraith–Ruprai Algorithm for Discrete Logarithms with Improved Complexity. In *Designs, Codes and Cryptography 87(5)*.

Topic 10: Rigorous analyses of Pollard's algorithms

10.1 Rigorous analyses of Pollard's rho

[HV02] Jeremy Horwitz and Ramarathnam Venkatesan. Random Cayley Digraphs and the Discrete Logarithm. In *ANTS 2002*.

[MV06] Stephen D. Miller and Ramarathnam Venkatesan. Spectral Analysis of Pollard Rho Collisions. In *ANTS 2006*.

[KMT07] Jeong Han Kim, Ravi Montenegro, and Prasad Tetali. Near Optimal Bounds for Collision in Pollard Rho for Discrete Log. In *FOCS 2007*.

[KMPT08] Jeong Han Kim, Ravi Montenegro, Yuval Peres, and Prasad Tetali. A Birthday Paradox for Markov Chains with an Optimal Bound for Collision in the Pollard Rho Algorithm for Discrete Logarithm. In *ANTS 2008*.

[BDJ14] Joppe W. Bos, Alina Dudeanu, and Dimitar Jetchev. Collision Bounds for the Additive Pollard Rho Algorithm for Solving Discrete Logarithms. In *Journal of Mathematical Cryptology 8(1)*.

10.2 Rigorous analyses of Pollard's kangaroo

[MT09] Ravi Montenegro and Prasad Tetali. How Long Does it Take to Catch a Wild Kangaroo? In *STOC 2009*.

Topic 11: Low Hamming weight discrete logarithm

*[Stinson02] Douglas R. Stinson. Some Baby-Step Giant-Step Algorithms for the Low Hamming Weight Discrete Logarithm Problem. In *Mathematics of Computation 71(237)*.

[KC08] Sungwook Kim and Jung Hee Cheon. A Parameterized Splitting System and Its Application to the Discrete Logarithm Problem with Low Hamming Weight Product Exponents. In *PKC 2008*.

[KPH17] Bailey Kacsmar, Sarah Plosker, and Ryan Henry. Computing Low-Weight Discrete Logarithms. In *SAC 2017*.

[EM20] Andre Esser and Alexander May. Low Weight Discrete Logarithms and Subset Sum in $2^{0.65n}$ with Polynomial Memory. In *EUROCRYPT 2020*.